

Entangling and assisted entangling power of bipartite unitary operations

Lin Chen^{1,2,*} and Li Yu^{3,†}

¹*School of Mathematics and Systems Science, Beihang University, Beijing 100191, China*

²*International Research Institute for Multidisciplinary Science, Beihang University, Beijing 100191, China*

³*National Institute of Informatics, 2-1-2 Hitotsubashi, Chiyoda-ku, Tokyo 101-8430, Japan*

(Dated: October 27, 2016)

Nonlocal unitary operations can create quantum entanglement between distributed particles, and the quantification of created entanglement is a hard problem. It corresponds to the concepts of entangling and assisted entangling power when the input states are, respectively, product and arbitrary pure states. We analytically derive them for Schmidt-rank-two bipartite unitary and some complex bipartite permutation unitaries. In particular, the entangling power of permutation unitary of Schmidt rank three can take only one of two values: $\log_2 9 - 16/9$ or $\log_2 3$ ebits. The entangling power, assisted entangling power and disentangling power of $2 \times d_B$ permutation unitaries of Schmidt rank four are all 2 ebits. These quantities are also derived for generalized Clifford operators. We further show that any bipartite permutation unitary of Schmidt rank greater than two has entangling power greater than 1.223 ebits. We construct the generalized controlled-NOT (CNOT) gates whose assisted entangling power reaches the maximum. We quantitatively compare the entangling power and assisted entangling power for general bipartite unitaries, and study their connection to the disentangling power. We also propose a probabilistic protocol for implementing bipartite unitaries.

PACS numbers: 03.65.Ud, 03.67.Lx, 03.67.Mn

I. INTRODUCTION

In quantum physics, nonlocal unitary operations can create and annihilate entanglement. Bipartite nonlocal unitary operations and entanglement are, respectively, a basic type of operation and a basic type of resource for implementing quantum information processing tasks and studying fundamental problems, such as quantum computing and steering [1]. The bipartite nonlocal unitary operation U on system A and B is a unitary gate that is not the tensor product of any two local unitary gates, i.e., $U \neq V_A \otimes W_B$. In other words, U has *Schmidt rank* greater than one. The entanglement of a bipartite pure state $|\psi\rangle_{AB}$ is defined as the von Neumann entropy $S(\cdot)$ of the reduced density matrix on any one system,

$$E(|\psi\rangle_{AB}) := S(\text{Tr}_A |\psi\rangle\langle\psi|). \quad (1)$$

In this paper we investigate the following problem: How is the entanglement of a bipartite pure state quantitatively changed under the action of a bipartite nonlocal unitary gate [2–8]? Here the state is referred to as the *input state* and contains ancilla systems that are not directly subject to the gate. Bipartite unitaries may create more entanglement than that of the input state. The maximum amount of entanglement increase over all input states is a lower bound of the entanglement cost for implementing bipartite unitaries under local operations and classical communications (LOCC). Our main motivation for studying the entangling capabilities of bi-

partite unitaries is to try to get insight on the following question, which we think belongs to the class of questions on (ir)reversibility of resources in quantum computation.

Is there a bipartite unitary such that its entanglement cost is strictly greater than its ability to create entanglement?

In the following we formalize the notion of the “ability to create entanglement” by introducing two types of entangling powers, and their technical definitions are given in Sec. I A. [The term “entanglement cost” also has a few different definitions; see the text around (5) and the formalized question stated after it.] The first type of entangling power is when the input state is restricted to a product pure state; and for the second type, the input state is an arbitrary pure state. Both types allow the input state to be on both the systems directly subject to the action of the unitary and some ancillary systems. The two types are respectively called the *entangling power* [2] and the *assisted entangling power*. Another quantity we consider is called the disentangling power [3], which is the maximum amount of entanglement decrease over all input states (allowing ancillary systems) as a result of applying the unitary. These three quantities are some of the most fundamental physical quantities to evaluate the usefulness of bipartite unitaries. Note that we do not discuss another type of entangling power which has also appeared in the literature [9, 10]. This is the average output entanglement (under a specific entanglement measure) over Haar random product input states without ancillae.

To investigate our problem, we study the above three quantities in terms of some classes of bipartite unitaries. They include the Schmidt-rank-two bipartite unitaries, the bipartite complex permutation unitaries of Schmidt

*Electronic address: lincen@buaa.edu.cn

†Electronic address: yupapers@sina.com

U	Sch U	$K_E(U)$	$K_{Ea}(U)$	$K_d(U)$
$d_A \times d_B$ unitaries	2	Lemma 9, Proposition 10, Lemma 21.	Partial result by Proposition 19	$K_{Ea}(U)$ by Lemma 25
$d_A \times d_B$ permutation unitaries	3	$\log_2 9 - 16/9$ or $\log_2 3$ ebits by Proposition 13	Partial result by Proposition 19	$K_{Ea}(U)$ by Proposition 26
$d_A \times d_B$ complex permutation unitaries	3	Partial result by Lemma 12	Partial result by Proposition 19	$K_{Ea}(U)$ by Proposition 26
$2 \times d_B$ complex permutation unitaries	3	Proposition 15	Partial result by Proposition 19	$K_{Ea}(U)$ by Proposition 26
$2 \times d_B$ complex permutation unitaries	4	2 ebits by Proposition 17	2 ebits by Theorem 24	2 ebits by Theorem 24
GCNOT	2	1 ebit by Proposition 20	1 ebit by Proposition 20	1 ebit by Proposition 20
generalized Clifford operators	no requirement	Proposition 22	Proposition 22	Proposition 22
$d_A \times d_B$ permutation unitaries	greater than two	> 1.223 ebits by Proposition 18	> 1.223 ebits by (5) and Proposition 18	> 1.223 ebits by (4) and Proposition 18
a family of non-controlled unitaries	no requirement	Proposition 16	?	$K_{Ea}(U^\dagger)$ by (4)

TABLE I: List of the main results of this paper in terms of the type of bipartite unitary U . The symbols Sch U , $K_E(U)$, $K_{Ea}(U)$, and $K_d(U)$ represent, respectively, the Schmidt rank of U , the entangling power of U , the assisted entangling power of U , and the disentangling power of U . The generalized CNOT (GCNOT) gate is defined in Sec. IV A. The “?” means unknown.

rank three or four, the generalized CNOT gates, and the bipartite generalized Clifford operators. The importance of these gates is summarized as follows. Bipartite unitaries of Schmidt rank two or three are locally equivalent to controlled unitary operators [7, 11, 12]. They include the basic ingredients of quantum computing such as CNOT gates and controlled-phase gates. The controlled unitary can be implemented with LOCC and a maximally entangled state [13], and is the mostly realizable class of nonlocal unitaries by experiments. The equivalence between bipartite and controlled unitaries has also been used to evaluate the delocalization power of bipartite unitaries [8]. As the investigation of bipartite unitaries of greater Schmidt rank is more involved, we focus on the permutation unitary gates. They have a simpler structure than that of arbitrary unitaries and contain experimentally realizable gates such as the SWAP gate. Any bipartite permutation unitary of Schmidt rank three can be implemented using LOCC and two ebits [6]. On the other hand, a protocol for implementing bipartite permutation unitaries of any Schmidt rank r has been given, by using $O(r)$ ebits of entanglement and $O(r)$ bits of classical communication [6]. The Clifford gates are central for the field of quantum error correction [14], and are interesting for many other topics in quantum information theory.

Our main results are concluded in Table I and introduced as follows. We analytically derive the entangling power of Schmidt-rank-two unitaries, and the results are

mainly presented in Lemma 9 and Proposition 10. In Proposition 13, we show that the entangling power of bipartite permutation unitary gates of Schmidt rank three can only take one of two values: $\log_2 9 - 16/9$ or $\log_2 3$ ebits. The result is counter-intuitive because one may expect that the entangling power depends on the gate more strongly. We are not aware of a similarly large family of bipartite unitary gates that have exactly two distinct values of entangling power. We analytically construct the gates for the value $\log_2 9 - 16/9$. The value $\log_2 3$ is the upper bound of entangling power of all Schmidt-rank-three bipartite unitaries. Next, we show in Proposition 17 that the entangling power of any $2 \times d_B$ complex bipartite permutation unitary of Schmidt rank four is 2 ebits, and in Proposition 18 that any bipartite permutation unitary of Schmidt rank greater than two has entangling power greater than 1.223 ebits. So permutation unitaries generally have a stronger entangling power and assisted entangling power than that of arbitrary bipartite unitaries, since the latter could approach zero. Third, we construct the notion of a generalized CNOT (GCNOT) gate and study its entangling power in Proposition 20. The GCNOT gate has the maximum entangling and assisted entangling power among Schmidt-rank-two bipartite unitaries of high dimensions. So the GCNOT gate plays the same role as the CNOT gate does in the two-qubit unitary gates. Fourth, we construct the notion of generalized Clifford operators and derive their entangling power, assisted entangling power and disentangling

power in Proposition 22. It turns out that they are all equal to the Schmidt strength defined in [2] and (7).

Other results in Table I are introduced in sections. Below we introduce the discussed quantities in terms of their physical meaning and mathematical formulation.

A. Definitions and physical meanings

The entangling power of a bipartite unitary U acting on the Hilbert space \mathcal{H} of systems A, B is defined as [2]

$$K_E(U) := \max_{|\alpha\rangle, |\beta\rangle} E(U(|\alpha\rangle|\beta\rangle)). \quad (2)$$

Here $|\alpha\rangle$ and $|\beta\rangle$ are pure states on system AR_A and BR_B , respectively, R_A and R_B are local ancillae, and the E is the von Neumann entropy of the reduced density matrix on one of the two systems AR_A and BR_B . So $|\alpha, \beta\rangle$ and $U|\alpha, \beta\rangle$ are bipartite states. For two bipartite unitaries U, V , both acting on \mathcal{H} , we have $K_E(U \otimes V) \geq K_E(U) + K_E(V)$. From [2], the collective use of U, V might have a stronger entangling power than the sum of that of U and V . This can even happen when $U = V$. Thus, the K_E is not, in general, weakly or strongly additive [2]. This is analogous to the superadditivity of various types of capacities of quantum channels [15, 16].

The entangling power needs a product state as the input state, so we do not need entanglement as the initial resource. This is a more efficient way from the point of view of experiments, because entanglement is usually hard to realize in a laboratory. On the other hand from the theoretical point of view, adding the entanglement as an initial resource may increase the entanglement that can be generated by the bipartite unitary. For this purpose we introduce the assisted entangling power. It also gives a lower bound for the entanglement cost under LOCC. The *assisted entangling power* of a bipartite unitary U is defined as

$$K_{Ea}(U) := \sup_{|\psi\rangle} \left(E(U(|\psi\rangle)) - E(|\psi\rangle) \right). \quad (3)$$

Here $|\psi\rangle$ is a bipartite pure state on the systems AR_A and BR_B , R_A and R_B are local ancillae, and the E is the von Neumann entropy of the reduced density matrix on one of the two systems AR_A and BR_B . The assisted entangling power has been discussed in the name of “entangling capacity” [17], and another definition without ancillae is also discussed in [17]. On the other hand, the quantity $K_{\Delta E}(U) := \sup_{|\psi\rangle} |E(U(|\psi\rangle)) - E(|\psi\rangle)|$ defined in [2] is lower bounded by $K_{Ea}(U)$. From the definition of weak additivity in [2], and the definitions of K_E and K_{Ea} , it can be deduced that if $K_{Ea} = K_E$ for some class of bipartite unitaries, then K_E is weakly additive for them. It is shown in [2] that K_E is strictly subadditive for some two-qubit unitaries, thus $K_E(U) < K_{Ea}(U)$ for some U . Numerical evidence in [17] also supports the same statement.

The introduction of ancillae R_A, R_B is necessary for both definitions of K_E and K_{Ea} . For example, the SWAP gate on two qubits cannot create any entanglement starting from a pure state on AB ; however, one can easily show that $K_E(\text{SWAP}) = 2$ ebits. When the ancillae are not allowed, denote the restricted versions of K_E and K_{Ea} as \bar{K}_E and \bar{K}_{Ea} , respectively. The paragraph after Eq. (12b) of [18] implies that there is a U such that $\bar{K}_{Ea}(U) > \bar{K}_E(U)$. This fact is also proved in [17].

If the expression $E(U(|\psi\rangle)) - E(|\psi\rangle)$ is changed to $E(|\psi\rangle) - E(U(|\psi\rangle))$ in (3), the resulting quantity $K_d(U)$ is the so-called *disentangling power* [3]. One can show that

$$K_d(U) = K_{Ea}(U^\dagger), \quad (4)$$

and determine the properties of disentangling power via that of assisted entangling power. The disentangling power physically means the maximum entanglement that a bipartite unitary can annihilate. The disentangling power and assisted entangling power are generally different. In page 3 of [3], a 2×3 non-controlled bipartite unitary U has been constructed so that $K_{Ea}(U) = K_E(U) = 2 > K_{Ea}(U^\dagger)$. Since $K_{Ea}(U^\dagger) \geq K_E(U^\dagger)$, we have $K_E(U) > K_E(U^\dagger)$. It solves an open problem in [2, Table 1].

As the physical inverse of entangling power, we investigate the cost of creating bipartite unitaries. In this paper, the “entanglement cost” of a bipartite unitary U is defined as $E_c(U) = \inf_p E_c(p)$, where p is any one-shot exact deterministic LOCC protocol for implementing U with a pure entangled state as the nonlocal resource, and $E_c(p)$ is the amount of entanglement in the resource state, measured using the entanglement entropy. The Schmidt rank of the pure state and the dimension of ancillary space are finite in the protocol p , and have no constant upper bound when taking the infimum. We refer to $E_c(U)$ as the one-shot entanglement cost. Define the asymptotic entanglement cost of a bipartite unitary U as $E'_c(U) := \lim_{n \rightarrow \infty} \frac{E_c(U^{\otimes n})}{n}$ and asymptotic assisted entangling power as $K'_{Ea}(U) := \lim_{n \rightarrow \infty} \frac{K_{Ea}(U^{\otimes n})}{n}$. Since entanglement is non-increasing under LOCC, we have $E'_c(U) \geq K'_{Ea}(U)$. The definitions of the two types of entanglement costs and the definition of assisted entangling power imply $K'_{Ea}(U) \geq K_{Ea}(U)$ and $E'_c(U) \leq E_c(U)$. We have

$$K_E(U) \leq K_{Ea}(U) \leq K'_{Ea}(U) \leq E'_c(U) \leq E_c(U). \quad (5)$$

Hence, if $K_E(U) = E_c(U)$ then all quantities become the same. This is exactly the case of generalized Clifford operators we investigate in Proposition 22. The question stated near the beginning of the introduction can be formalized as the following question: Is there a bipartite unitary U , such that $K_{Ea}(U) < E_c(U)$?

The rest of this paper is organized as follows. In Sec. II we introduce the notations and known results used in the paper. In Sec. III we investigate the entangling power of bipartite unitaries of Schmidt rank

two, bipartite permutation unitaries, and $2 \times d_B$ complex permutation matrices of Schmidt rank three. We also investigate non-controlled bipartite unitaries including Schmidt-rank-four $2 \times d_B$ complex permutation unitaries and two-qubit unitaries. We further show the connection between our results and symmetric informationally complete positive operator-valued measure (SIC-POVM). In Sec. IV we investigate the assisted entangling power of bipartite unitaries. We derive the entangling power and assisted entangling power for generalized Clifford operators. We also present the concept of generalized CNOT gate. Such gates have the maximum entangling power in arbitrary dimensions. In Sec. V we study the relation between the entangling power, assisted entangling power and the disentangling power. In Sec. VI we discuss two conjectures arising in the literature and this paper. We conclude in Sec. VII.

II. PRELIMINARIES

In this section we introduce the notations and known results used in the paper. Denote the computational-basis states of the bipartite Hilbert space $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B$ by $|i, j\rangle, i = 1, \dots, d_A, j = 1, \dots, d_B$. Let I_A and I_B be the identity operators on the spaces \mathcal{H}_A and \mathcal{H}_B , respectively. We also denote I_d and 0_d respectively as the identity and zero matrix of order d . Any bipartite unitary gate U acting on \mathcal{H} has *Schmidt rank* [denoted as $\text{Sch}(U)$] equal to n if there is an expansion of the form $U = \sum_{j=1}^n A_j \otimes B_j$ where the $d_A \times d_A$ matrices A_1, \dots, A_n are linearly independent, and the $d_B \times d_B$ matrices B_1, \dots, B_n are also linearly independent. The Schmidt rank is equivalent to the notion of operator-Schmidt rank in [2, 19]. The above expansion is called the *Schmidt decomposition*. We can further write the Schmidt decomposition in a standard form,

$$U = \sum_{j=1}^r c_j A_j \otimes B_j, \quad (6)$$

where $\frac{1}{d_A} \text{Tr}(A_j^\dagger A_k) = \frac{1}{d_B} \text{Tr}(B_j^\dagger B_k) = \delta_{jk}$, $c_j > 0$, and $\sum_{j=1}^r c_j^2 = 1$. Then we introduce the *Schmidt strength*

$$K_{\text{Sch}}(U) = - \sum_{j=1}^r c_j^2 \log_2 c_j^2 \quad (7)$$

which is used as a measure of the “nonlocal content” of U [2]. The inequality

$$\log_2 \text{Sch}(U) \geq K_E(U) \geq K_{\text{Sch}}(U) \quad (8)$$

holds for any bipartite unitary U in terms of the definition of K_E and [2, Theorem 1].

Next, U is a *controlled unitary gate*, if U is equivalent to $\sum_{j=1}^{d_A} |j\rangle\langle j| \otimes U_j$ or $\sum_{j=1}^{d_B} V_j \otimes |j\rangle\langle j|$ via local unitaries. To be specific, U is a controlled unitary from A or B

side, respectively. In particular, U is controlled in the computational basis from A side if $U = \sum_{j=1}^{d_A} |j\rangle\langle j| \otimes U_j$. Bipartite unitary gates of Schmidt rank two or three are in fact controlled unitaries [7, 11, 12]. We shall denote $V \oplus W$ as the ordinary direct sum of two matrices V and W , and $V \oplus_B W$ as the direct sum of V and W from the B side (called “ B -direct sum”). In the latter case, V and W respectively act on two subspaces $\mathcal{H}_A \otimes \mathcal{H}'_B$ and $\mathcal{H}_A \otimes \mathcal{H}''_B$, respectively, such that $\mathcal{H}'_B \perp \mathcal{H}''_B$. A permutation matrix (or called “permutation unitary”) is a unitary matrix containing elements 0 and 1 only. A partial permutation matrix is obtained by changing some element 1 to 0 in a permutation matrix. A bipartite controlled-permutation matrix is a permutation matrix controlled in the computational basis of one system. Each term in a controlled-permutation unitary refers to a term of the form $P \otimes V$ (or with the two sides swapped), where P is a projector whose rank is a positive integer, and V is a local permutation unitary. A “big row” of the $d_A d_B \times d_A d_B$ unitary matrix U refers to a $d_B \times d_A d_B$ submatrix given by ${}_A\langle j|U$, for some $j \in \{1, \dots, d_A\}$. Similarly, a “big column” of U refers to a $d_A d_B \times d_B$ submatrix given by $U|j\rangle_A$, for some $j \in \{1, \dots, d_A\}$. A “block” of U refers to a $d_B \times d_B$ submatrix given by ${}_A\langle j|U|k\rangle$, for some $j, k \in \{1, \dots, d_A\}$, and when $j = k$, the block is called a “diagonal block.”

It is known that any controlled unitary controlled from the A side on the space $\mathcal{H}_A \otimes \mathcal{H}_B$ is locally equivalent to

$$U = \sum_{j=1}^m P_j \otimes U_j \quad (9)$$

where the P_j ’s are pairwise orthogonal projectors on \mathcal{H}_A , and the U_j ’s are unitary operators on \mathcal{H}_B . We can further assume that the U_j ’s are pairwise linearly independent, and say that U is controlled with m terms. Next we review mathematical results on von Neumann entropy, quantum channel, and controlled unitaries.

A. Mathematics of quantum information

Let $H(\{p_j\}) := \sum_j -p_j \log_2 p_j$ be the Shannon entropy of the probability distribution $\{p_j\}$. The following lemma (i) is known as the subadditivity of von Neumann entropy. It follows from the paragraph below (11.73) and Exercise 11.16 of [20]. Lemma 1 (ii) is from (11.84) and Theorem 11.10 in [20]. In particular the second inequality in (11) is known as the concavity of von Neumann entropy.

Lemma 1 (i) Let ρ_{AB} be a density operator on two systems A, B . Then

$$|S(\rho_A) - S(\rho_B)| \leq S(\rho_{AB}) \leq S(\rho_A) + S(\rho_B). \quad (10)$$

The first equality holds if and only if there is a split of the system $A = A_1 A_2$ such that $\rho_{AB} = |\psi\rangle\langle\psi|_{A_1 B} \otimes \sigma_{A_2}$, or there is a split of the system $B = B_1 B_2$ such that

$\rho_{AB} = |\psi\rangle\langle\psi|_{AB_1} \otimes \sigma_{B_2}$. The second equality holds if and only if $\rho_{AB} = \rho_A \otimes \rho_B$.

(ii) Let $\{p_j\}$ be a probability distribution of $p_j > 0$ and $\{\rho_j\}$ a set of density operators. Then

$$\sum_j p_j S(\rho_j) + H(\{p_j\}) \geq S(\sum_j p_j \rho_j) \geq \sum_j p_j S(\rho_j). \quad (11)$$

The first equality holds if and only if the range of ρ_i and ρ_j are pairwise orthogonal, $\forall i, j$. The second equality holds if and only if $\rho_i = \rho_j$, $\forall i, j$. \square

We will use this lemma to derive the entangling power of bipartite complex permutation unitaries of Schmidt rank three in Proposition 15, and investigate the assisted entangling power of controlled unitaries in Proposition 19. Below is a known result from the majorization theory.

Lemma 2 Let ρ and σ be two quantum states. If the spectrum of ρ is strictly majorized by the spectrum of σ , i.e., $\rho \prec_s \sigma$, then $S(\rho) > S(\sigma)$.

We will use the lemma to derive the upper bound of entangling power of a family of bipartite unitary operator of Schmidt rank three in Lemma 12. Let $|\psi\rangle = \sum_{j=1}^r \sqrt{p_j} |a_j, b_j\rangle$ be the Schmidt decomposition with nonnegative real numbers p_j in the descending order. We refer to the vector $\text{sv}(\psi)$ of probability distribution (p_1, \dots, p_r) as the *Schmidt vector* of $|\psi\rangle$. For an arbitrary vector x of probability distribution, we refer to $\text{des}(x)$ as the vector whose elements are the same as those of x except that they are in the descending order. Next we show conditions by which a quantum channel converts an arbitrary input into the maximally mixed state.

Lemma 3 For d^2 operators K_1, \dots, K_{d^2} and an invertible operator R acting on \mathbf{C}^d , the following five assertions are equivalent:

- (i) $\text{Tr} K_i^\dagger R^{-1} K_j = \delta_{ij}$ for $i, j = 1, \dots, d^2$;
- (ii) $\sum_{j=1}^{d^2} K_j^\dagger X K_j = (\text{Tr} R X) I_d$ for all matrices X acting on \mathbf{C}^d ;
- (iii) $\sum_{j=1}^{d^2} K_j^\dagger X K_j = (\text{Tr} R X) I_d$ for all pure states X acting on \mathbf{C}^d ;
- (iv) $\text{Tr}_A(\sum_{j=1}^{d^2} |j\rangle\langle j| \otimes K_j^\dagger) Y (\sum_{j=1}^{d^2} |j\rangle\langle j| \otimes K_j) = \text{Tr}(R \cdot \text{Tr}_A Y) I_d$ for all bipartite operators Y acting on $\mathcal{H} = \mathbf{C}^{d^2} \otimes \mathbf{C}^d$;
- (v) $\text{Tr}_A(\sum_{j=1}^{d^2} |j\rangle\langle j| \otimes K_j^\dagger) Y (\sum_{j=1}^{d^2} |j\rangle\langle j| \otimes K_j) = \text{Tr}(R \cdot \text{Tr}_A Y) I_d$ for all pure product states Y acting on $\mathcal{H} = \mathbf{C}^{d^2} \otimes \mathbf{C}^d$.

Proof. The equivalence between assertions (i) and (ii) is from [21, Proposition 3]. Assertion (iii) is equivalent to (ii) because the equation $\sum_{j=1}^{d^2} K_j^\dagger X K_j = (\text{Tr} R X) I_d$ is linear with X , and any matrix space is spanned by rank-one positive semidefinite matrices. The same reason implies the equivalence between (iv) and (v). Finally,

(ii) and (iv) are equivalent by setting $X = \text{Tr}_A Y$. This completes the proof. \square

An important case of this lemma is when $R = I_d$.

Corollary 4 For d^2 operators K_1, \dots, K_{d^2} acting on \mathbf{C}^d , the following five assertions are equivalent:

- (i) $\text{Tr} K_i^\dagger K_j = \delta_{ij}$ for $i, j = 1, \dots, d^2$;
- (ii) $\sum_{j=1}^{d^2} K_j^\dagger X K_j = (\text{Tr} X) I_d$ for all matrices X acting on \mathbf{C}^d ;
- (iii) $\sum_{j=1}^{d^2} K_j^\dagger X K_j = I_d$ for all pure states X acting on \mathbf{C}^d ;
- (iv) $\text{Tr}_A(\sum_{j=1}^{d^2} |j\rangle\langle j| \otimes K_j^\dagger) Y (\sum_{j=1}^{d^2} |j\rangle\langle j| \otimes K_j) = (\text{Tr} Y) I_d$ for all bipartite operators Y acting on $\mathcal{H} = \mathbf{C}^{d^2} \otimes \mathbf{C}^d$;
- (v) $\text{Tr}_A(\sum_{j=1}^{d^2} |j\rangle\langle j| \otimes K_j^\dagger) Y (\sum_{j=1}^{d^2} |j\rangle\langle j| \otimes K_j) = I_d$ for all pure product states Y acting on $\mathcal{H} = \mathbf{C}^{d^2} \otimes \mathbf{C}^d$.

The corollary is used in the following discussion. Assertion (i) implies that the set $\{K_j\}_{j=1, \dots, d^2}$ is an orthonormal basis of the $d \times d$ matrix space under the Hilbert-Schmidt inner product $\|A, B\|_{hs} := \text{Tr}(A^\dagger B)$. It occurs e.g., when $\{\frac{K_j}{\sqrt{d}}\}_{j=1, \dots, d^2}$ is the Heisenberg-Weyl (HW) group. In this case, assertion (ii) implies [20, Exercise 11.19]. Furthermore, assertion (ii) implies that the map $\Lambda(\cdot) := \frac{1}{d^3} \sum_{j=1}^{d^2} K_j^\dagger(\cdot) K_j$ is a depolarized channel and at the same time a unital channel because of $\Lambda(I) = I$ [22]. The unital channels have been extensively studied in the past years [23–25]. In particular, the unitaries K_j have been used to construct mutually unbiased unitaries [26]. The following result is implied by [27]. See more general cases in [28, 29].

Lemma 5 Let $U = \sum_{j=1}^{d_A} |j\rangle\langle j| \otimes U_j$ be a controlled unitary such that there is a constant state $|\alpha\rangle$ satisfying that for any state $|\beta\rangle$, $U|\alpha\rangle_A |\beta\rangle_B$ is maximally entangled. Then $d_A \geq d_B^2$.

Since $d_A \geq d_B^2 \geq d_B$, $U|\alpha\rangle_A |\beta\rangle_B$ is locally equivalent to the $d_B \times d_B$ maximally entangled state. The condition of this lemma is equivalent to the statement that there is a constant state $|\alpha\rangle = \sum_{j=1}^{d_A} \sqrt{p_j} |j\rangle$, such that $\sum_{j=1}^{d_A} p_j U_j |\beta\rangle\langle\beta| U_j^\dagger = \frac{1}{d_B} I_B$. If $d_A = d_B^2$, then this equation is a special case of Corollary 4 (iii). Since it is equivalent to Corollary 4 (i), we can work out that $p_j = \frac{1}{d_B^2}$ for any j . Hence, $\{U_j\}$ must be a set of orthogonal unitary bases under the Hilbert-Schmidt inner product. The following fact is mentioned in the paragraph of [30, Eq. (15)].

Lemma 6 For any $d \times d$ matrix X , the matrix $\frac{1}{r} \sum_{k=0}^{r-1} U_k X U_k^\dagger$ is diagonal when either of the following two conditions is satisfied:

- (i) $r = d$ and $U_k = \text{diag}(1, \omega^k, \dots, \omega^{k(r-1)})$ and $\omega = e^{2\pi i/d}$;
- (ii) $r = 2^d$ and $U_k = \text{diag}(\pm 1, \pm 1, \dots, \pm 1)$.

The above two lemmas will be used to characterize the entangling power of bipartite unitaries below Lemma 8. If either condition holds, then one can find out d permutation matrices $P_k := \sum_{j=1}^d |j\rangle\langle 1 + (j + k - 1) \bmod d|$ for $k = 1, \dots, d$ and $Y_i := P_i(\frac{1}{r} \sum_{k=0}^{r-1} U_k X U_k^\dagger) P_i^\dagger$. Then $\sum_{i=1}^d Y_i = (\text{Tr} X) I_d$, i.e., any matrix X can be converted to the maximally mixed state under the unital channel. If the condition is (i), then one can verify that the set $\{\frac{1}{\sqrt{d}} P_i U_k\}$ satisfies Corollary 4 (i). So the set is a constructive example of the operators in Corollary 4. On the other hand, if the condition is (ii) then the set does not satisfy Corollary 4 (i).

Finally we present a lemma for the block-controlled unitary (BCU) operations [11]. The latter is defined as the direct sum of two bipartite unitaries from the A or B side (allowing the freedom of local unitaries). So a controlled unitary is a BCU and the inverse is wrong. The BCU is the generalization of the notion of controlled unitaries. The Lemma 7 below will be used to show that any bipartite permutation unitary of Schmidt rank greater than two has entangling power greater than 1.223 ebits; see Proposition 18. We also define the *block-controlled-permutation unitary* (BCPU) as a BCU which is block diagonal in the standard basis on the controlling side and is at the same time a permutation unitary in the standard basis. This notion will be used in the proof of Proposition 18.

Lemma 7 *Let $U = V \oplus_B W$ be a bipartite unitary. Then $K_E(U) \geq \max\{K_E(V), K_E(W)\}$.*

Proof. By the equation $U = V \oplus_B W$, we have $\mathcal{H}_B = \mathcal{H}_B^V \oplus \mathcal{H}_B^W$, where the subspace \mathcal{H}_B^V (respectively, \mathcal{H}_B^W) is the input subspace of V (respectively, W). Denote the input state on BR_B as $|\phi\rangle_{BR_B}$. The inequality follows by restricting the reduced density matrix $\text{Tr}_{R_B}(|\phi\rangle\langle\phi|_{BR_B})$ to have support in the subspaces \mathcal{H}_B^V and \mathcal{H}_B^W , respectively. This completes the proof. \square

III. ENTANGLING POWER OF BIPARTITE UNITARIES

Two main classes of bipartite unitary operations are bipartite controlled unitaries and permutation unitaries. The former contains the basics of quantum circuits, such as CNOT gates and controlled-phase gates. Next, any bipartite unitary is the product of controlled unitaries [31, 32]. Any bipartite controlled unitary can be implemented with LOCC and a maximally entangled state [13], thus a general bipartite unitary can be implemented by performing the controlled unitaries in its decomposition. The implementation is more efficient for bipartite unitaries of Schmidt rank at most three, because they are equivalent to controlled unitaries under local unitaries [7, 11, 12]. In particular, any bipartite permutation unitary of Schmidt rank three can be implemented using LOCC and two ebits [6]. On the other hand, a protocol

for implementing bipartite permutation unitaries of any Schmidt rank r has been given, by using $O(r)$ ebits of entanglement and $O(r)$ bits of classical communication [6]. These facts imply that the two classes of bipartite unitaries are experimentally available resources. So the next step is to understand their entangling power in practice.

We begin by studying the entangling power of bipartite controlled unitaries in Lemma 8, and then apply it to some well-known bipartite unitaries in subsections. The latter includes Schmidt-rank-two unitaries in Sec. III A, Schmidt-rank-three permutation unitaries and $2 \times d_B$ complex permutation matrices in Sec. III B, and non-controlled bipartite unitaries such as a family of bipartite unitaries including the SWAP gate as a proper subset, and Schmidt-rank-four $2 \times d_B$ complex permutation unitaries in Sec. III C. We further show that any bipartite permutation unitary of Schmidt rank greater than two has entangling power greater than 1.223 ebits in Proposition 18. We also point out the connection between the controlled unitaries and the symmetric informationally complete positive operator-valued measure (SIC-POVM) in Sec. III D.

If $|\alpha, \beta\rangle$ maximizes $E(U(|\alpha\rangle|\beta\rangle))$ in (2), then we call it the critical state of U . In general, a bipartite unitary has many critical states. The critical states of bipartite controlled unitaries have a simpler structure, as we show below.

Lemma 8 *Suppose $U = \sum_{j=1}^m P_j \otimes U_j$ in (9) is a controlled unitary controlled with m terms. Then (i)*

$$\begin{aligned} K_E(U) &= \max_{|\alpha\rangle \in \mathcal{H}_A, |\beta\rangle \in \mathcal{H}_{BR_B}} E(U(|\alpha\rangle|\beta\rangle)) \\ &= \max_{p_j \geq 0, \sum_{j=1}^m p_j = 1, |\beta\rangle \in \mathcal{H}_{BR_B}} S\left(\sum_{j=1}^m p_j (U_j)_B |\beta\rangle\langle\beta|_{BR_B} (U_j)_B^\dagger\right) \\ &\leq \log_2 \text{Sch}(U) \\ &\leq \log_2 \min\{m, d_B^2\}. \end{aligned} \quad (12)$$

In particular, $K_E(U) = \log_2 \text{Sch}(U)$ if and only if $\sum_{j=1}^m p_j (U_j)_B |\beta\rangle\langle\beta|_{BR_B} (U_j)_B^\dagger$ is a normalized projector of rank $\text{Sch}(U)$.

(ii) If U is also controlled from the B side, then

$$\begin{aligned} K_E(U) &= \max_{|\alpha\rangle \in \mathcal{H}_A, |\beta\rangle \in \mathcal{H}_B} E(U(|\alpha\rangle|\beta\rangle)) \\ &= \max_{p_j \geq 0, \sum_{j=1}^m p_j = 1, |\beta\rangle \in \mathcal{H}_B} S\left(\sum_{j=1}^m p_j (U_j)_B |\beta\rangle\langle\beta|_B (U_j)_B^\dagger\right) \\ &\leq \log_2 \text{Sch}(U). \end{aligned} \quad (13)$$

In particular, $K_E(U) = \log_2 \text{Sch}(U)$ if and only if $\sum_{j=1}^m p_j (U_j)_B |\beta\rangle\langle\beta|_B (U_j)_B^\dagger$ is a normalized projector of rank $\text{Sch}(U)$.

(iii) If U is not controlled from the B side, then

$$K_E(U) \geq \max_{|\alpha\rangle \in \mathcal{H}_A, |\beta\rangle \in \mathcal{H}_B} E(U(|\alpha\rangle|\beta\rangle)), \quad (14)$$

and the inequality may hold or not.

(iv) Let $|\alpha, \beta\rangle$ be the critical state of U . Then $|\alpha\rangle$ can be chosen as a linear combination of the computational basis states with non-negative coefficients. If all U_j are diagonal, then $|\beta\rangle \in \mathcal{H}_B$ can be chosen to also possess the same property.

The proof is given in Appendix A. Assertion (i) implies that the ancilla in the controlling side of a controlled unitary cannot increase the entangling power of the unitary. Note that an upper bound of the entanglement cost of controlled unitary from the A side with $d_A = 2, 3$ is $\log_2 \min\{d_A^2, d_B\}$ [11]. It is similar to that in (i), which is an upper bound of the entangling power. The entangling power is upper bounded by the entanglement cost with two upper bounds, namely $\log_2 \min\{d_A^2, d_B\}$ and $\min\{\log_2 \text{Sch}(U), \log_2 d_A, 2 \log_2 d_B\}$. On the other hand, the trivial upper bound $K_E(U) \leq \log_2 \text{Sch}(U)$ is again obtained in spite of the simplification by the controlled unitaries. A tighter upper bound might be achievable only if the considered controlled unitaries are restricted to a smaller subset of controlled unitaries.

Next, assertion (ii) implies that the unitary is controlled from both sides; then we can discard both ancillae in (2). For example, the critical state of a Schmidt-rank-two unitary [7], or a Schmidt-rank-three diagonal unitary need not include any ancilla system. On the other hand, for controlled unitaries U whose B side cannot be the controlling system, the ancilla system R_B in (12) cannot generally be removed because of (iii).

The first example in (iii) is not a permutation matrix. Here we give an example of permutation matrix. Let $V = \sum_{j=1}^4 |j\rangle\langle j| \otimes P_j$, where $P_1 = I_3$, $P_2 = |1\rangle\langle 1| + |2\rangle\langle 3| + |3\rangle\langle 2|$, $P_3 = |2\rangle\langle 2| + |3\rangle\langle 1| + |1\rangle\langle 3|$, and $P_4 = |3\rangle\langle 3| + |1\rangle\langle 2| + |2\rangle\langle 1|$ act on the space \mathcal{H}_{AB} . So V is a bipartite permutation matrix. One can show by calculation that $V(\frac{1}{2\sqrt{3}} \sum_{j=1}^4 |j\rangle_A \otimes \sum_{k=1}^3 |kk\rangle_{B R})$ has entanglement more than $\log_2 3$ ebits, which is the upper bound of the entangling power of V without an ancilla. Hence, the inequality in Eq. (14) holds for V .

Suppose U in Lemma 5 is also controlled from the B side. If the “constant” in Lemma 5 is removed, then the condition of this lemma means that $S\left(\sum_{j=1}^{d_A} p_j(U_j)_B |\beta\rangle\langle\beta|_B (U_j)_B^\dagger\right) = \log_2 \min\{d_A, d_B\}$. So the upper bound in (13) is saturated, and the equation $d_A \geq d_B^2$ might no longer hold. On the other hand, we do not know the case when U in Lemma 5 is not controlled from the B side.

If the unitaries U_i in (13) are those in either case of Lemma 6, then we can work out that $K_E(U) = \log d_B$. In the following subsections, we investigate several types of bipartite unitaries and analytically derive their entangling power using Lemma 8.

A. Schmidt-rank-two unitaries

In this subsection we provide the analytical method of computing the entangling power of Schmidt-rank-two bipartite unitaries U . It is known [7] that up to local unitaries, U is a controlled unitary and can be written as the form

$$U = P \otimes I_{d_B} + (I_A - P) \otimes D \quad (15)$$

where P is a projector, and $D = \text{diag}(e^{i\theta_1}, \dots, e^{i\theta_{d_B}})$ is a diagonal unitary with real $\theta_1, \dots, \theta_{d_B} \in [0, 2\pi)$ in the ascending order. It suffices to work with U in the above form because the entangling power is invariant up to local unitaries. Lemma 8 (ii) implies that

$$K_E(U) = \max_{p \in [0,1], |\beta\rangle = (b_1, \dots, b_{d_B})^T, b_j \geq 0} S\left(p|\beta\rangle\langle\beta| + (1-p)D|\beta\rangle\langle\beta|D^\dagger\right), \quad (16)$$

where the components $b_j \geq 0$ follow from the fact that the von Neumann entropy is invariant up to unitaries. Let V be a $d_B \times d_B$ unitary whose first row is (b_1, \dots, b_{d_B}) . Applying the same fact to (16) we obtain

$$\begin{aligned} K_E(U) &= \max_{p \in [0,1], |\beta\rangle = (b_1, \dots, b_{d_B})^T, b_j \geq 0} S\left(pV|\beta\rangle\langle\beta|V^\dagger + (1-p)VD|\beta\rangle\langle\beta|D^\dagger V^\dagger\right) \\ &= \max_{p \in [0,1], |\beta'\rangle = (x, \sqrt{1-x^2})^T, x = |\sum_j e^{i\theta_j} b_j^2|, b_j \geq 0, \sum_j b_j^2 = 1} S\left(p|0\rangle\langle 0| + (1-p)|\beta'\rangle\langle\beta'|\right). \end{aligned} \quad (17)$$

The maximum is achievable if and only if the determinant of the 2×2 matrix in the last row of (17) reaches the maximum. It implies $p = 1/2$. Using (16) we have

$$K_E(U) = \max_{b_1, \dots, b_{d_B}, \sum_j b_j^2 = 1} H\left(\frac{1 - |\sum_j e^{i\theta_j} b_j^2|}{2}, \frac{1 + |\sum_j e^{i\theta_j} b_j^2|}{2}\right). \quad (18)$$

Setting $c_j = b_j^2$, we have $\sum_j c_j = 1$. Hence,

$$\begin{aligned} \left|\sum_j e^{i\theta_j} b_j^2\right| &= \left[\left(\sum_j c_j \cos \theta_j\right)^2 + \left(\sum_j c_j \sin \theta_j\right)^2\right]^{\frac{1}{2}} \\ &= \left[\sum_j c_j^2 + 2 \sum_{j>k} c_j c_k \cos(\theta_j - \theta_k)\right]^{\frac{1}{2}} \\ &= \left[1 - 2 \sum_{j>k} c_j c_k + 2 \sum_{j>k} c_j c_k \cos(\theta_j - \theta_k)\right]^{\frac{1}{2}} \\ &= \left[1 - 4 \sum_{j>k} c_j c_k \sin^2\left(\frac{\theta_j - \theta_k}{2}\right)\right]^{\frac{1}{2}}. \end{aligned} \quad (19)$$

So the minimum of $|\sum_j e^{i\theta_j} b_j^2|$, equivalently $K_E(U)$ in (18), is reached at the maximum of $y(\{c_j\}) := \sum_{j>k} c_j c_k \sin^2(\frac{\theta_j - \theta_k}{2})$, where the parameters $c_j \geq 0$ and $\sum_j c_j = 1$. If $d_B = 2$, then straightforward computation shows that $K_E(U)$ in (18) is reached when $c_1 = c_2 = \frac{1}{2}$. We have the following.

Lemma 9 *Any $d_A \times 2$ controlled unitary $U = P_1 \otimes I_2 + P_2 \otimes \text{diag}(e^{i\theta_1}, e^{i\theta_2})$ with orthogonal projectors P_1, P_2 and the real parameter θ has the entangling power $K_E(U) = H(\frac{1 - |\cos \frac{\theta_1 - \theta_2}{2}|}{2}, \frac{1 + |\cos \frac{\theta_1 - \theta_2}{2}|}{2})$.*

If $d_A = 2$, then the lemma reduces to the result in [2, Theorem 2]. In particular, the entangling power of two-qubit controlled unitaries is the same as the Schmidt strength in terms of Theorem 2 of [2]. Lemma 9 thus provides the analytical formula for the Schmidt strength of two-qubit controlled unitaries. On the other hand, Lemma 9 implies that $K_E(U)$ reaches the maximum 1 ebit if and only if $\theta_1 - \theta_2 = (2k + 1)\pi$ for $k \in \mathbf{Z}$. When $d_A = 2$ the gate U is locally equivalent to the CNOT gate. Besides, (18) for $d_B = 2$ also generalizes the result in [2].

Next, if $d_B > 2$, then we use the equations $\frac{\partial(y(\{c_j\}) + \lambda(\sum_j c_j - 1))}{\partial c_j} = 0$ where λ is the Lagrange multiplier. One can show that at most two of these equations are independent. So we have $\lambda = -1/2$, and thus $\sum_j c_j \sin^2(\frac{\theta_1 - \theta_j}{2}) = \frac{1}{2}$, $\sum_j c_j \sin^2(\frac{\theta_2 - \theta_j}{2}) = \frac{1}{2}$, and $\sum_j c_j = 1$. For given θ_j we can derive the set of roots c_j of the above linear equations. On the other hand, we need to study the boundary case. By setting some $c_j = 0$ in (18) we can similarly obtain the above equations and work out the remaining c_j . They give rise to another set of roots c_j . Repeating this procedure, we obtain a few different sets of roots c_j . We input these sets in the binary function in (18) and obtain corresponding output values. The maximum of these values is equal to $K_E(U)$. So we can analytically work out $K_E(U)$. For example, using the above arguments and $h(i, j) := H(\frac{1 - |\cos \frac{\theta_i - \theta_j}{2}|}{2}, \frac{1 + |\cos \frac{\theta_i - \theta_j}{2}|}{2})$ we can derive the entangling power of U with $d_B = 3$.

Proposition 10 *Let U be (15) with $d_B = 3$. We have $K_E(U) = \max\{h(1, 2), h(2, 3), h(1, 3)\}$.*

This result and Lemma 9 show the following conjecture for $n = 2, 3$.

Conjecture 11 *For the Schmidt-rank-two bipartite unitary $V = |1\rangle\langle 1| \otimes I_n + |2\rangle\langle 2| \otimes \sum_{j=1}^n e^{i\theta_j} |j\rangle\langle j|$, we have $K_E(V) = \max_{1 \leq i < j \leq d_B} \{h(i, j)\}$.*

Using the results in this subsection, we further study the maximum of entangling and assisted entangling power of Schmidt-rank-two bipartite unitaries, namely the generalized CNOT gates in Sec. IV A.

B. Schmidt-rank-three permutation unitaries

Finding the entangling power of an arbitrary Schmidt-rank-three bipartite unitary is a technically involved problem. We investigate the permutation operations. They are controlled unitaries [12] though are not always controlled permutation unitaries. The main result is presented in Proposition 13 and was proposed as an open problem in [6]. We further derive the entangling power of Schmidt-rank-three $2 \times d_B$ permutation operations in Proposition 15. First we present a preliminary lemma proved in Appendix B.

Lemma 12 *Consider the bipartite unitary operator of Schmidt rank three,*

$$\begin{aligned} U &= D_1 \otimes I_B \\ &+ D_2 \otimes (I_m \oplus I_n \oplus V_1) \\ &+ D_3 \otimes (I_m \oplus V_3 \oplus I_q), \end{aligned} \quad (20)$$

where D_j are nonzero and satisfy $D_j D_k = \delta_{jk} D_j$, $\sum_j D_j = I_A$, and V_1 and V_3 are respectively of size $q \times q$ and $n \times n$. Then $K_E(U) \leq \log_2 9 - 16/9$ ebits. The equality is saturated when U is a permutation unitary.

The considered U is a special case of the bipartite unitaries

$$\begin{aligned} &D_1 \otimes I_B \\ &+ D_2 \otimes (I_m \oplus I_n \oplus V_1 \oplus V_2) \\ &+ D_3 \otimes (I_m \oplus V_3 \oplus I_q \oplus V_4), \end{aligned} \quad (21)$$

where D_j are nonzero and $D_j D_k = \delta_{jk} D_j$, $\sum_j D_j = I_A$, and V_1, V_2, V_3 , and V_4 are permutation matrices. V_1 and V_3 are, respectively, of size $q \times q$ and $n \times n$, and both V_2 and V_4 are of size $p \times p$ where $p = d_B - m - n - q$. If V_1 or V_3 contains a nonzero diagonal entry, then we can move the entry by local permutation matrices on \mathcal{H}_B so that I_m is replaced with I_{m+1} . So V_1 and V_3 do not contain any nonzero diagonal entry. Similarly, we may assume that V_2 and V_4 do not have a nonzero diagonal entry in the same column when $p > 0$. Now we state the main result of this subsection.

Proposition 13 *The entangling power of any bipartite permutation unitary of Schmidt rank three can only take one of two values: $\log_2 9 - 16/9$ or $\log_2 3$ ebits. The former occurs if and only if the unitary is of the form of (21) and $p = 0$.*

Proof. Let U be the bipartite permutation unitary of Schmidt rank three in the assertion. It was shown in the proof of [6, Proposition 1] that if U is not of the form (21), then the entangling power of U is exactly $\log_2 3$ ebits. The same conclusion holds when U is of the form of (21) and $p > 0$. It remains to prove the assertion when U is of the form of (21) and $p = 0$. This is a special case of Lemma 12 where U is a permutation unitary; thus,

$K_E(U) = \log_2 9 - 16/9$ ebits. This completes the proof. \square

To generalize this result, we derive $K_E(U)$ when U is a complex permutation unitary on the $2 \times d_B$ system. We present the following lemma, which is clear.

Lemma 14 *Let $U = \sum_{j,k=1}^2 |j\rangle\langle k| \otimes U_{jk}$ be a $2 \times d_B$ complex permutation unitary of Schmidt rank three. Then either $U_{11} \propto U_{22}$ or $U_{12} \propto U_{21}$.*

Up to local permutation unitaries, we may assume that $U_{11} = U_{22} = I_n \oplus 0_{d_B-n}$, $U_{12} = 0_n \oplus I_{d_B-n}$, and $U_{21} = 0_n \oplus C$ where C is a complex permutation unitary of order $d_B - n$. Let the entangling power of $|1\rangle\langle 2| \otimes I_B + |2\rangle\langle 1| \otimes C$ be M . This leads us to the following proposition.

Proposition 15

$$K_E(U) = H\left(\frac{1}{e^M + 1}, \frac{e^M}{e^M + 1}\right) + \frac{e^M}{e^M + 1} M. \quad (22)$$

The proof is given in Appendix C. By computation we can show that $K_E(U)$ monotonically increases with M . So $K_E(U)$ reaches its lower and upper bound, respectively, at $M = 0$ and $M = 1$, hence $1 \leq K_E(U) \leq 1.57100011... < \log_2 3 \approx 1.585$ (ebits). So any $2 \times d_B$ complex permutation unitary of Schmidt rank three cannot reach the maximum. We qualitatively explain this result as follows. Let us first consider the case that the initial state on BR_B is a maximally entangled state. When the initial state on AR_A is a maximally entangled state, there are two terms among the four terms in the output state that are proportional to each other on the BR_B side, e.g., the terms corresponding to U_{11} and U_{22} in the case $U_{11} \propto U_{22}$, so in the Schmidt decomposition of the output state, the three terms are not of equal weight; hence, the entangling power is less than $\log_2 3$ ebits. The case of other initial states on AR_A are also similar because the two terms from V are of less weight than the remaining term. Finally, the case of other initial states on BR_B is also similar.

We remark that since there are only two 2×2 permutation unitary matrices I_2 and σ_x , the $d_A \times 2$ controlled-permutation unitary has Schmidt rank of at most two. So any $d_A \times 2$ Schmidt-rank-three bipartite unitary, which may be a permutation unitary, is not locally equivalent to a controlled-permutation unitary.

C. Non-controlled bipartite unitaries

In previous subsections we have investigated the entangling power of Schmidt-rank-two bipartite unitaries and Schmidt-rank-three bipartite permutation matrices. They are both controlled unitaries, while we often deal with more non-controlled unitaries in practice. This is a harder problem and we investigate four examples. In the first example, we compute the entangling power of a special bipartite unitary in Proposition 16. The unitary includes the bipartite SWAP gate of arbitrary dimensions.

Next we show that any $2 \times d_B$ complex permutation unitary of Schmidt rank four has entangling power 2 ebits in Proposition 17. We further show in Proposition 18 that any bipartite permutation unitary of Schmidt rank greater than two has entangling power greater than 1.223 ebits. Finally, we investigate two-qubit unitaries.

The first example is a family of bipartite unitaries on $d_A \times d_B$ space with $d_A \leq d_B$,

$$U_{AB} = \sum_{j,k=1}^{d_A} |j\rangle\langle k| \otimes V_{jk}, \quad (23)$$

where the $d_B \times d_B$ submatrices V_{jk} satisfy the following two properties: (1) for any given k , the value $\text{Tr} V_{jk}^\dagger V_{jk}$ is either zero or constant c_k , and (2) if we put the entries of them in the same $d_B \times d_B$ matrix, then any two entries are in different positions of the matrix. Suppose V_{jk} and $V_{j'k'}$ are nonzero blocks and $|\psi\rangle = \frac{1}{\sqrt{d_B}} \sum_{i=1}^{d_B} |i\rangle_B |i\rangle_{R_B}$ is a maximally entangled state of Schmidt rank d_B on BR_B , where R_B is an ancillary system. The properties imply that the two non-normalized states $V_{jk}|\psi\rangle$ and $V_{j'k'}|\psi\rangle$ have the same modulus and are orthogonal. If we perform U_{AB} on the non-normalized input state $(\sum_k \frac{1}{\sqrt{c_k}} |kk\rangle)_{AR_A} |\psi\rangle_{BR_B}$, then we obtain a maximally entangled state of Schmidt rank $\text{Sch}(U_{AB})$. Thus $K_E(U) \geq \log_2 \text{Sch}(U_{AB})$ (ebits). On the other hand, by Lemma 8 we have $K_E(U) \leq \log_2 \text{Sch}(U_{AB})$. We conclude the above argument as follows.

Proposition 16 *For unitaries of the form (23) we have $K_E(U_{AB}) = \log_2 \text{Sch}(U_{AB})$.*

Note that (23) may be not a complex permutation matrix. An example is the 2×3 bipartite unitary

$$U_{AB} = \begin{bmatrix} 1/\sqrt{2} & 0 & 0 & 0 & 0 & 1/\sqrt{2} \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 1/\sqrt{2} & 0 & 0 & 0 & 0 & -1/\sqrt{2} \\ 0 & 0 & 1 & 0 & 0 & 0 \end{bmatrix}. \quad (24)$$

The example satisfies that c_k is constant for all k . In this case it is easy to verify that $K_E(U_{AB}^\dagger) = K_E(U_{AB}) = \log_2 \text{Sch}(U_{AB})$ ebits, and the input state is the same as before.

In the second example, we investigate the entangling power of the $2 \times d_B$ permutation unitary U . If it has Schmidt rank two or three, then $K_E(U)$ has been respectively derived in Lemma 9 and Proposition 15. So it suffices to investigate the Schmidt-rank-four case.

Proposition 17 *Any $2 \times d_B$ complex permutation unitary of Schmidt rank four has entangling power of 2 ebits.*

Proof. Let U be a $2 \times d_B$ complex permutation unitary of Schmidt rank four. Up to local complex permutation

unitaries, we may assume that $U = \sum_{j,k=1}^2 |j\rangle\langle k| \otimes U_{jk}$ where $U_{11} = I_k \oplus 0_{d_B-k}$, $0 < k < d_B$, and the zero columns (if any) among the rightmost $d_B - k$ columns of U_{12} are in the rightmost columns of U_{12} . If a zero column exists, then there are four integers $i \in [1, k]$, $j \in [k+1, d_B-k]$ and $m, n \in [1, d_B]$, $m \neq n$, such that U contains four nonzero entries in the positions $|1, i\rangle\langle 1, i|$, $|1, j\rangle\langle 2, i|$, $|2, m\rangle\langle 1, d_B|$, and $|2, n\rangle\langle 2, d_B|$. By performing U on the input state $\frac{1}{\sqrt{2}}(|11\rangle + |22\rangle)_{ARA} \frac{1}{\sqrt{2}}(|i, i\rangle + |d_B, d_B\rangle)_{BRB}$, we obtain a uniformly entangled state of Schmidt rank four. So the assertion holds. On the other hand, if the rightmost $d_B - k$ columns of U_{12} do not contain a zero column, up to local complex permutation unitaries we can assume that $U_{12} = 0_k \oplus 1_{d_B-k}$. Since U has Schmidt rank four, there are five integers $i \in [1, k]$, $j \in [k+1, d_B-k]$, and $m, n, p \in [1, d_B]$, $p \neq i$ and $m \neq n$, such that U contains four nonzero entries in the positions $|1, i\rangle\langle 1, i|$, $|1, m\rangle\langle 2, j|$, $|2, n\rangle\langle 1, j|$, and $|2, p\rangle\langle 2, i|$. By performing U on the input state $\frac{1}{\sqrt{2}}(|11\rangle + |22\rangle)_{ARA} \frac{1}{\sqrt{2}}(|ii\rangle + |jj\rangle)_{BRB}$, we obtain a uniformly entangled state of Schmidt rank four. So the assertion holds. This completes the proof. \square

We have investigated the entangling power of many sorts of permutation unitaries. Below, we investigate the lower bound of entangling power of all permutation unitaries. The proof is given in Appendix D.

Proposition 18 *Any bipartite permutation unitary of Schmidt rank greater than two has entangling power of greater than 1.223 ebits.*

The result shows that the entangling power of permutation unitaries is generally greater than that of arbitrary bipartite unitaries, because the latter with any Schmidt rank could have entangling power close to zero. An example of such bipartite unitaries is the controlled unitary $\sum_{j=1}^{d_A} |j\rangle\langle j| \otimes U_j$, where the linearly independent U_j are close to the identity matrix.

Finally, we estimate the entangling power of two-qubit unitaries. It is known [2] that any two-qubit unitary gate is locally equivalent to $U = c_0 I_2 \otimes I_2 + c_x \sigma_x \otimes \sigma_x + c_y \sigma_y \otimes \sigma_y + c_z \sigma_z \otimes \sigma_z$ with complex numbers c_0, c_x, c_y and c_z . We perform U on the product states $\frac{1}{\sqrt{2}}(|11\rangle + |22\rangle)_{ARA} \otimes |\psi\rangle_{BRB}$, where $|\psi\rangle_{BRB}$ is an arbitrary two-qubit state. The resulting state is locally equivalent to $|\Psi\rangle = \sum_{j=0,x,y,z} c_j |a_j, \psi_j\rangle$, where $|a_j\rangle$ is an orthonormal basis in \mathbb{C}^4 . It follows from [33, Corollary 4] that $\text{sv}(\psi) \succ \text{des}(|c_0|^2, |c_x|^2, |c_y|^2, |c_z|^2)$. It follows from Lemma 2 that $H(\text{sv}(\psi)) \leq H(|c_0|^2, |c_x|^2, |c_y|^2, |c_z|^2)$. The equality is achievable when $|\psi\rangle$ is the two-qubit maximally entangled state. So we obtain $K_E(U) \geq \sum_{j=0,x,y,z} -|c_j|^2 \log_2 |c_j|^2$. This result is exactly [2, Theorem 1], and the right-hand side of this equation is equal to the Schmidt strength. The result also coincides with (7). It is believed that the strict inequality holds for some U .

D. Connection with SIC-POVM

In a d -dimensional Hilbert space, the SIC-POVM [34] consists of d^2 outcomes that are subnormalized projectors onto pure states $\frac{1}{d}|\psi_j\rangle\langle\psi_j|$ for $j = 1, \dots, d^2$, such that $|\langle\psi_j|\psi_k\rangle|^2 = \frac{1+d\delta_{jk}}{d+1}$. Hence $\sum_{j=1}^{d^2} |\psi_j\rangle\langle\psi_j| = dI_d$. Many known SIC-POVMs are generated by performing the Heisenberg-Weyl (HW) group $\{U_j\}_{j=1, \dots, d^2}$ on the so-called fiducial state $|\varphi\rangle$ such that $|\psi_j\rangle = U_j|\varphi\rangle$ and $|\langle\varphi|U_j|\varphi\rangle| = \frac{1}{\sqrt{d+1}}$, where $U_j \neq I_d$. In the following we relate the SIC-POVM to (13) in Lemma 8. If the U_j in (13) form the HW group, $|\beta\rangle$ in (13) is a fiducial vector, $d_A = d_B^2$, then we can set $p_j = \frac{1}{d^2}$ in (13) for all j and obtain $K_E(U) = \log_2 d_B$ because of $|\psi_j\rangle = U_j|\varphi\rangle$. Physically, it means that the reduced density operator on B for the output state of the U in (13) can always be chosen to be the maximally mixed state for some suitable input state. As far as we know, this is the first necessary condition of the existence of fiducial-state-generated SIC-POVM in terms of the entangling power of controlled unitaries. On the other hand, if the fiducial-state-generated SIC-POVM does not exist in some \mathbb{C}^d , the last equality in (13) still holds when $d_A = d_B^2$, in terms of Corollary 4. So the above necessary condition may be not sufficient, though we do not know the existence of SIC-POVM. An interesting question is whether the “fiducial-state-generated” can be removed from the above discussion. It is an open problem whether the existence of SIC-POVM in \mathbb{C}^d implies the existence of fiducial-state-generated SIC-POVM in \mathbb{C}^d [35], though the converse evidently holds.

IV. ASSISTED ENTANGLING POWER OF BIPARTITE UNITARIES

In this section we investigate the assisted entangling power of bipartite unitaries. By definition, the input states can be arbitrary pure states with reference systems. Hence, the derivation of assisted entangling power is a harder problem than that of entangling power. In Proposition 19, we construct the upper bound for the assisted entangling power of controlled unitaries, and the necessary and sufficient condition by which the bound is saturated. Further, we introduce two families of (non-controlled) bipartite unitaries: the generalized CNOT gates in Sec. IVA and the generalized Clifford gates in Sec. IVB. The GCNOT gate has the maximum entangling and assisted entangling power among Schmidt-rank-two bipartite unitaries of high dimensions. So the GCNOT gate plays the same role as the CNOT gate does in the two-qubit unitary gates. We will derive the entangling power and assisted entangling power of both gates in Propositions 20 and 22, respectively. Further, the asymptotic entangling and assisted entangling power, and the disentangling power of Clifford gates are also derived in Proposition 22.

Proposition 19 Suppose $U = \sum_{j=1}^m P_j \otimes U_j$ in (9) is a controlled unitary controlled with m terms. Then (i)

$$\begin{aligned} & \log_2 m \\ & \geq K_{Ea}(U) \\ & = \max_{\sum_{j=1}^m M_j = \rho \in \mathcal{S}(\mathcal{H}_{BRB}), M_j \geq 0, \text{Tr} \rho = 1} S \left[\sum_{j=1}^m (U_j \otimes I_{R_B}) M_j (U_j^\dagger \otimes I_{R_B}) \right] - S(\rho) \\ & \geq K_E(U). \end{aligned} \quad (25)$$

(ii) The first inequality in (25) becomes the equality if and only if there is a mixed state $\sigma \in \mathcal{S}(\mathcal{H}_B)$, such that the equations $\text{Tr}(\sigma U_j^\dagger U_k) = 0$ hold for any j, k and $j > k$.

Further, σ can be chosen as diagonal if the U_i are all diagonal. σ can be chosen as real if the U_i are all real.

(iii) $K_{Ea}(U)$ and $K_E(U)$ are both equal to $\log_2 m$ or not at the same time. If they are equal to $\log_2 m$ then the ρ achieving the maximum in (25) can be chosen as a pure state.

(iv) Let $V = \sum_{j=1}^m Q_j \otimes U_j$ be a controlled unitary on \mathcal{H} , where the Q_j are pairwise orthogonal projectors or zero projectors. Then

$$\log_2 m \geq \log_2 \text{Sch}(U) \geq K_E(U) \geq K_E(V), \quad (26)$$

$$\log_2 m \geq K_{Ea}(U) \geq K_{Ea}(V). \quad (27)$$

The last equality in both equations hold when all Q_j are nonzero.

The proof is given in Appendix E. If the U_i in (25) are all diagonal then $U_i \otimes I_{R_B}$ commutes with the controlled unitary $W = \sum_i |i\rangle\langle i| \otimes V_i$ acting on $\mathcal{H}_B \otimes \mathcal{H}_{R_B}$ with any unitary V_i . The maximum in (25) does not change if we replace $S \left[\sum_{j=1}^m (U_j \otimes I_{R_B}) M_j (U_j^\dagger \otimes I_{R_B}) \right] - S(\rho)$ with $S \left[W \sum_{j=1}^m (U_j \otimes I_{R_B}) M_j (U_j^\dagger \otimes I_{R_B}) W^\dagger \right] - S(W \rho W^\dagger)$. Since there is no confusion, we can still name $W M_j W^\dagger$ as M_j , and $W \rho W^\dagger$ as ρ . By choosing a suitable W , we can assume that the $d_{R_B} \times d_{R_B}$ diagonal blocks of any given M_k are all diagonal.

The argument in (25) for the maximum can be replaced with $S(\rho) - S \left[\sum_{j=1}^m (U_j^\dagger \otimes I_{R_B}) M_j (U_j \otimes I_{R_B}) \right]$. It is realized by replacing M_j by $(U_j^\dagger \otimes I_{R_B}) M_j (U_j \otimes I_{R_B})$ in (25).

We have shown in Proposition 19 (ii) that the ρ by which the first inequality becomes the equality can be chosen as a pure state. For general ρ the proof of (ii) implies the equations $\langle \psi | (U_j^\dagger U_k \otimes I_{R_B}) | \varphi \rangle = 0$ for any $|\psi\rangle, |\varphi\rangle \in \mathcal{R}(\rho)$. Note that $\text{rank } \rho = \text{Dim } \mathcal{R}(\rho) = \text{Dim} \left((U_j^\dagger U_k \otimes I_{R_B}) \mathcal{R}(\rho) \right)$. If $\text{rank } \rho \geq \lfloor \frac{d_B d_{R_B}}{2} \rfloor + 1$, then the two subspaces $\mathcal{R}(\rho)$ and $(U_j^\dagger U_k \otimes I_{R_B}) \mathcal{R}(\rho)$ intersect. So the equation cannot be satisfied. Hence, we have $\text{rank } \rho \leq \lfloor \frac{d_B d_{R_B}}{2} \rfloor$.

The condition $\text{Tr}(\sigma U_j^\dagger U_k) = 0$ in Proposition 19 (ii) cannot be satisfied when $\text{Sch}(U) := r < m$. To explain this fact, without loss of generality we may assume that U_1, \dots, U_r are linearly independent, and U_{r+1} is the linear combination of them. Then the condition implies that $\text{Tr} \sigma = 0$, which gives us a contradiction. So the first inequality in (25) is strict when $\text{Sch}(U) < m$. The inequality may be still strict when $\text{Sch}(U) = m$. An example is the U whose U_j are roughly equal to each other. In this case the assisted entangling power $K_{Ea}(U)$ could approach zero.

As another example, we consider the permutation unitary U in Lemma 12. The condition $\text{Tr}(\sigma U_j^\dagger U_k) = 0$ is equivalent to the equations

$$\text{Tr}(\sigma(I_m \oplus I_n \oplus V_1)) = 0, \quad (28)$$

$$\text{Tr}(\sigma(I_m \oplus V_3 \oplus I_q)) = 0, \quad (29)$$

$$\text{Tr}(\sigma(I_m \oplus V_3^\dagger \oplus V_1)) = 0. \quad (30)$$

The complex conjugate of the second equation, plus the first equation and minus the last equation results in $\text{Tr} \sigma = 0$. This is a contradiction with the mixed state σ , and thus $\text{Tr}(\sigma U_j^\dagger U_k) = 0$ cannot be satisfied. So $\log_2 3 > K_{Ea}(U) \geq K_E(U) = \log_2 9 - 16/9$ ebits by Lemma 12. We do not know whether the inequality in $K_{Ea}(U) \geq K_E(U)$ holds for this class of U .

Next, it follows from Lemma 8 that $\log_2 m$ is also the upper bound of $K_E(U)$. Proposition 19 (iii) implies that if the bound is achievable then the entangling power and assisted entangling power are both equal to $\log_2 d_m$. It can be realized by studying the conditions in Lemma 8.

Finally, Proposition 19 (iv) does not restrict the rank of Q_i . It also implies that if $K_E(V) = \log_2 \text{Sch}(U)$ then the last two equalities in (26) hold. For example, the 5×2 controlled unitary

$$\begin{aligned} U = & |1\rangle\langle 1| \otimes I_2 + |2\rangle\langle 2| \otimes \sigma_x + |3\rangle\langle 3| \otimes \sigma_z \\ & + |4\rangle\langle 4| \otimes \left(\frac{\sigma_x + \sigma_z}{\sqrt{2}} \right) + |5\rangle\langle 5| \otimes \left(\frac{iI_2 + \sigma_x}{\sqrt{2}} \right) \end{aligned} \quad (31)$$

has Schmidt rank three. Since $V = |1\rangle\langle 1| \otimes I_2 + |2\rangle\langle 2| \otimes \sigma_x + |3\rangle\langle 3| \otimes \sigma_z$ has entangling power $\log_2 3$, so does U . So we have provided a method of computing the entangling power of controlled unitaries whose Schmidt rank is smaller than the maximum of d_A and d_B . In the following two subsections, we give two families of bipartite unitaries whose assisted entangling power can be analytically derived.

A. Generalized CNOT gates

We have described in Proposition 19 when a controlled unitary gate has the maximum entangling and assisted entangling power. In this subsection we investigate the simplest case, namely $m = 2$ in Proposition 19. Let $\theta_1, \dots, \theta_{d_B}$ be real numbers such that the vector $(e^{i\theta_1}, \dots, e^{i\theta_{d_B}})$ is orthogonal to a d_B -dimensional

nonzero vector whose components are zeros or positive numbers. Given a projector P of rank in $[1, d_A - 1]$, we say that the Schmidt-rank-two bipartite unitary gate $P \otimes I_B + (I_A - P) \otimes (\sum_{j=1}^{d_B} e^{i\theta_j} |j\rangle\langle j|)$ is a *generalized CNOT (GCNOT) gate* up to local unitaries. If $d_A = d_B = 2$, then the definition of θ_j 's implies that $(e^{i\theta_1}, e^{i\theta_2})$ is orthogonal to a two-dimensional nonzero vector whose components are zeros or positive numbers. Hence, $e^{i\theta_1} = -e^{i\theta_2}$. So the GCNOT gate reduces to the CNOT gate. Using these definitions and Proposition 19, we can generalize Lemma 21 of [6].

Proposition 20 *Let U be a Schmidt-rank-two bipartite unitary. Then the following conditions are equivalent.*

- (i) U is a GCNOT gate;
- (ii) $K_{Ea}(U) = 1$ ebit;
- (iii) $K_E(U) = 1$ ebit.

Proof. It is known that U is a controlled unitary [7]. Up to the exchange of systems and local unitaries we may assume that $U = \sum_{j=1}^2 P_j \otimes U_j$ as in (9). The equivalence between (ii) and (iii) follows from Proposition 19 (iii). Using local unitaries we may assume that $U_1 = I_B$ and U_2 is a diagonal unitary. It does not change the entangling and assisted entangling power of U . If (i) holds, then the definition of GCNOT gate implies that there is a diagonal density matrix σ such that $\text{Tr}(\sigma U_2) = 0$. So $K_E(U) = 1$ ebit in terms of Proposition 19 (ii). On the other hand, if (ii) holds, then Proposition 19 (ii) implies that there is a diagonal density matrix σ such that $\text{Tr}(\sigma U_2) = 0$. So U is a GCNOT gate. We have proved (ii) \rightarrow (i). This completes the proof. \square

The result shows that the GCNOT gate has the maximum entangling and assisted entangling power among Schmidt-rank-two bipartite unitaries of high dimensions. So the GCNOT gate plays the same role as the CNOT gate does in the two-qubit unitary gates. On the other hand, the GCNOT gate with dimension bigger than two contains parameters up to local unitaries, while the CNOT gate is constant. So the set of GCNOT gates contains more than one element, and this is a primary difference between the GCNOT and CNOT gates. Nevertheless, we do not know the difference between GCNOT gates in the same dimensions. On the other hand, the definition of GCNOT gates implies that if the dimension of a Schmidt-rank-two bipartite unitary is bigger, then it is more possible to become a GCNOT gate.

Proposition 19 shows that different controlled unitaries may have the same entangling and assisted entangling power, respectively. It helps derive them for more bipartite unitaries. For Schmidt-rank-two bipartite unitaries, we can simplify their structure by the following lemma.

Lemma 21 *Let $U = P \otimes I_B + (I_A - P) \otimes (\sum_j e^{i\theta_j} P_j)$ be a Schmidt-rank-two controlled unitary where P is a projector and P_j are orthogonal projectors. Let $V = |1\rangle\langle 1| \otimes I_n + |2\rangle\langle 2| \otimes \sum_j e^{i\theta_j} |j\rangle\langle j|$. Then $K_E(U) = K_E(V)$ and $K_{Ea}(U) = K_{Ea}(V)$.*

Proof. Let $W = |1\rangle\langle 1| \otimes I_B + |2\rangle\langle 2| \otimes (\sum_j e^{i\theta_j} P_j)$. By setting in the last statement of Proposition 19 (iv) the Q_j as rank-one projectors, we have $K_E(U) = K_E(W)$ and $K_{Ea}(U) = K_{Ea}(W)$. Up to the exchange of systems the last statement of Proposition 19 (iv) shows that $K_E(W) = K_E(V)$ and $K_{Ea}(W) = K_{Ea}(V)$. This completes the proof. \square

As a consequence of Lemma 21, we obtain a possible simplification for the proof of Conjecture 11: We need only consider the case that the $\theta_j \in [0, 2\pi)$ in the conjecture are pairwise different. Finally, the generalized GCNOT gates may be defined as $\sum_j |j\rangle\langle j| \otimes D_j$, where each D_j is a diagonal unitary such that $\text{Tr} D_j^\dagger D_k = 0$ for $j \neq k$. The existence of such gates is related to an open problem on the partial Hadamard matrices [36].

B. Generalized Clifford operators

In this subsection we derive the closed formula of assisted entangling power of bipartite Clifford operators. Let $\sigma_x, \sigma_y, \sigma_z$ be the usual 2×2 Pauli matrices. Define the Pauli group \mathcal{P}_n to be consisting of unitary operators on n qubits of the form $e^{ik\pi/2} \bigotimes_{j=1}^n \sigma_{a_j}$, where $a_j \in \{0, 1, 2, 3\}$, and $\sigma_0 = I_2$, $\sigma_1 = \sigma_x$, $\sigma_2 = \sigma_y$, and $\sigma_3 = \sigma_z$, and k is an integer. A unitary operator C on n qubits is a Clifford operator if and only if

$$CSC^\dagger \in \mathcal{P}_n, \quad \forall S \in \mathcal{P}_n. \quad (32)$$

For example, the one-qubit Hadamard gate and the two-qubit CNOT gate are Clifford gates, but the Tofolli gate on 3 qubits is not a Clifford gate. Almost all quantum gates are not Clifford gates. The generalized Pauli group on d -dimensional qudits can be defined as the group generated by the following two unitary operators [37]:

$$\begin{aligned} X &= \sum_{k=0}^{d-1} |(k-1) \bmod d\rangle\langle k|, \\ Z &= \sum_{k=0}^{d-1} e^{2\pi i k/d} |k\rangle\langle k|. \end{aligned} \quad (33)$$

Then the generalized Clifford operators are defined as those C which satisfy (32) when the \mathcal{P}_n is understood as the generalized Pauli group on n qudits.

It is claimed in [37] that the asymptotic entanglement cost for approximately implementing two-qudit generalized Clifford gates U (viewed as a bipartite unitary across the two qudits) is equal to the Schmidt strength of U . Better yet, the one-shot entanglement cost $E_c(U)$ for exactly implementing two-qudit generalized Clifford gates U is equal to $K_{Sch}(U)$, which can be obtained by a protocol as follows (it is mentioned in Protocol 7 of [38], but is known before, see e.g. a more general protocol in [39]): It is generalized from the protocol shown in [40, Fig. 2] by changing the target gate from a CNOT gate to any two-qudit Clifford gate, replacing the initial state $|\chi\rangle$ with

$\frac{1}{d} \sum_{j=1}^d \sum_{k=1}^d |j\rangle_a U(|j\rangle_A |k\rangle_B) |k\rangle_b$ (the systems a, A, B, b correspond to the four middle lines of [40, Fig. 2], in the up-to-down order), changing the local Bell measurements to generalized Bell measurements, and changing the Pauli gates to generalized Pauli gates. The reason such a protocol works is that the generalized Clifford operators map the generalized Pauli operators to the generalized Pauli operators. The two qudits here are assumed to be of equal dimension, since when the dimensions are unequal, we suspect there might not be a nontrivial Clifford group. More generally, the protocol can be extended to the case that the two input systems A and B contain m and n qudits of equal dimension d , respectively. We call the U in such general cases as a bipartite generalized Clifford operator. We have the following.

Proposition 22 *All bipartite generalized Clifford operators V satisfy that*

$$\begin{aligned} K_E(V) &= K_{Ea}(V) = K'_{Ea}(V) = E'_c(V) = E_c(V) \\ &= K_{Sch}(V) = K_d(V) = - \sum_{j=1}^r c_j^2 \log_2 c_j^2, \end{aligned} \quad (34)$$

where the positive constants c_j are uniquely decided by (6).

Proof. The equality $E_c(U) = K_{Sch}(U)$ in the above paragraph, together with (5), (7), and (8) imply the assertion except $K_d(V)$. Further, we have

$$K_d(V) = K_{Ea}(V^\dagger) = K_{Sch}(V^\dagger) = - \sum_{j=1}^r c_j^2 \log_2 c_j^2. \quad (35)$$

The first equality follows from the definition of disentangling power. The second equality in (35) follows from other equalities in (34) and the fact that V^\dagger is also a generalized Clifford operator; the latter follows from (32) because $CS_1C^\dagger = S_2$ is equivalent to $S_1 = C^\dagger S_2 C$, where C is a generalized Clifford operator and S_1, S_2 are generalized Pauli operators. The last equality in (35) follows from (6) and (7). This completes the proof. \square

V. RELATION BETWEEN ENTANGLING AND ASSISTED ENTANGLING POWER

We have investigated the entangling and assisted entangling power of bipartite unitaries in terms of the definitions in (2) and (3). An alternative definition of entangling power is to replace the product state in (2) with separable states, i.e., $\max_{p_j, |\alpha_j\rangle, |\beta_j\rangle} E'(\sum_j p_j U |\alpha_j, \beta_j\rangle \langle \alpha_j, \beta_j| U^\dagger)$, where E' is a bipartite entanglement measure of systems AR_A and BR_B . Many fundamental entanglement measures such as the entanglement of formation [41], the relative entropy of entanglement [42], and the geometric measure

of entanglement [43] are convex. If E' is one of these measures then we have

$$\begin{aligned} & \max_{p_j, |\alpha_j\rangle, |\beta_j\rangle} E'(\sum_j p_j U |\alpha_j, \beta_j\rangle \langle \alpha_j, \beta_j| U^\dagger) \\ & \leq \max_{p_j, |\alpha_j\rangle, |\beta_j\rangle} \sum_j p_j E'(U |\alpha_j, \beta_j\rangle \langle \alpha_j, \beta_j| U^\dagger) \\ & \leq \max_{|\alpha_j\rangle, |\beta_j\rangle} E'(U |\alpha_j, \beta_j\rangle \langle \alpha_j, \beta_j| U^\dagger) \\ & = K_E(U). \end{aligned} \quad (36)$$

The last equality follows from the fact that any entanglement measure reduces to the von Neumann entropy for bipartite pure states. Hence, the two definitions coincide in many cases and it suffices to use (2) for quantifying the entangling power of bipartite unitaries.

Next we quantitatively characterize (5).

Lemma 23 *Let $d_A \leq d_B$ and U a bipartite unitary. We have*

$$2 \log_2 d_A \geq K'_{Ea}(U) \geq K_{Ea}(U) \geq K_E(U), \quad (37)$$

and the two inequalities become equalities at the same time. When they are equalities, the input state can be chosen as a product state $|\Psi\rangle_{AR_A} \otimes |\Phi\rangle_{BR_B}$ where $|\Psi\rangle$ is the $d_A \times d_A$ maximally entangled state.

Proof. The last two inequalities in the assertion follow from (5). If the inequality $2 \log_2 d_A \geq K_{Ea}(U)$ holds, then $2 \log_2 d_A \geq K'_{Ea}(U)$ follows from the definition of $K'_{Ea}(U)$. The inequality holds because such number of ebits can implement U by teleporting the system of Alice to Bob, performing the U locally on Bob's side, and teleporting the output of system A back to Alice. This completes the proof. \square

Compared with the assisted entangling power, the asymptotic assisted entangling power is a tighter lower bound for the entanglement cost under LOCC. One can show that the inequalities in (37) become equalities when U is the $d_A \times d_A$ SWAP gate. In Proposition 19 for controlled unitaries U , we have shown a tighter upper bound of $K_{Ea}(U)$ than that in (37). So the first inequality in (37) can be strict. On the other hand, the last inequality in (37) can also be strict by the following argument which is based on [2, Theorem 3]. Let $U = \sqrt{1-p}I \otimes I + i\sqrt{p}X \otimes X$ for some $p \in [0, 1]$. The proof of [2, Theorem 3] shows that $K_E(U \otimes U) \geq H[(1-2p)^2]$, as well as the fact that $H[(1-2p)^2] > 2H(p)$ for some range of p . It is shown in the proof of [2, Theorem 2] that $K_E(U) = H(p)$. Hence, for p in some range, the strict inequality $K_E(U \otimes U) > 2K_E(U)$ holds, and by definition $K_{Ea}(U) \geq \frac{1}{2}K_E(U \otimes U)$; thus, for some two-qubit Schmidt-rank-two unitaries U , the strict inequality $K_{Ea}(U) > K_E(U)$ holds. Note that [2] does not mention this inequality (although the above argument means that this inequality is essentially implied by their analysis), but it remarks that the inequality $K_{\Delta E}(U) > K_E(U)$ holds for some U ; see the comment on [2, p5], which is

based on [2, Theorem 3]. The latter inequality is a weaker inequality because $K_{\Delta E}(U) \geq K_{Ea}(U)$ for any bipartite unitary U .

Next we investigate the disentangling power using Lemma 23.

A. Disentangling power

The example with different disentangling power and assisted entangling power in [3] is a Schmidt-rank-four 3×2 bipartite unitary. We show that many bipartite unitaries of smaller Schmidt rank have equal disentangling power and assisted entangling power. Note that the complex conjugate of a complex permutation unitary is still a complex permutation unitary. From Proposition 17 and Lemma 23 we get the following.

Theorem 24 *Any $2 \times d_B$ complex permutation unitary U of Schmidt rank four satisfies*

$$K_d(U) = K_{Ea}(U) = K_E(U) = 2 \quad (38)$$

ebits.

To construct more examples, we present a preliminary lemma. The definitions of $K_E(U)$ and $K_{Ea}(U)$ imply

$$\begin{aligned} K_E(U) &= K_E(U^*), \\ K_{Ea}(U) &= K_{Ea}(U^*), \end{aligned} \quad (39)$$

and thus we are led to the following lemma.

Lemma 25 *$K_E(U) = K_E(U^\dagger)$ and $K_{Ea}(U) = K_{Ea}(U^\dagger)$ holds when the bipartite unitary U is locally equivalent to U^\dagger or a symmetric matrix.*

For example, such U can be any two-qubit unitary, because it is the sum of the tensor product of Pauli operators. Next, U can also be any Schmidt-rank-two bipartite unitary because it is locally equivalent to the diagonal unitary. A nontrivial example is as follows.

Proposition 26 *Any Schmidt-rank-three $d_A \times 2$ bipartite unitary is locally equivalent to a symmetric matrix.*

Proof. Let U be a Schmidt-rank-three $d_A \times 2$ unitary. It is known that U is a controlled unitary [11]. Up to local unitaries we may assume that $U = \sum_{j=1}^{d_A} |j\rangle\langle j| \otimes U_j$ where U_j are all 2×2 unitary matrices, and the first three of them are linearly independent. Up to local unitaries on \mathcal{H}_B we may assume that $U_1 = I_2$ and U_2 is diagonal. Since U_3 is a 2×2 unitary, the non-diagonal entries of U_3 have the same modulus. We can perform suitable diagonal local unitaries to make the two entries equal to the modulus. Then the resulting U_1, U_2 and U_3 are all symmetric. Since any U_j is the linear combination of them, it is also symmetric. Hence, U is locally equivalent to a symmetric matrix. This completes the proof. \square

Equation (39) implies that performing the complex conjugate on any bipartite unitary operation does not change the entangling power, assisted entangling power, and disentangling power of this operation. This phenomenon could still hold for multipartite unitaries if we generalize the definition of the three powers to multipartite scenario. So we may regard the complex conjugate as a local operation for nonlocal unitaries U , though the U^* is generally not convertible to U via LOCC. Nevertheless, they are convertible via stochastic LOCC. Since U of Schmidt rank r can be used to generate a Schmidt-rank- r entangled state, which can be converted with some probability into a uniformly entangled state of Schmidt rank r implementing U^* probabilistically. We construct the protocol for the implementation in the next subsection.

B. A probabilistic protocol for implementing bipartite unitaries

Given a bipartite unitary U , we may assume $U = \sum_{j=1}^r c_j A_j \otimes B_j$, where r is the Schmidt rank of U , and $\text{Tr}(A_j^\dagger A_k) = \delta_{jk} = \text{Tr}(B_j^\dagger B_k)$, where δ is the Kronecker delta symbol, and c_j are positive coefficients. The unitarity condition $U^\dagger U = I_{AB}$ implies that

$$I_{AB} = \sum_{j,k=1}^r c_k^* c_j A_k^\dagger A_j \otimes B_k^\dagger B_j \quad (40)$$

Taking partial trace over system A , we have $I_B = \frac{1}{d_A} \sum_{j=1}^r c_j^2 B_j^\dagger B_j$. Similarly, $I_A = \frac{1}{d_B} \sum_{j=1}^r c_j^2 A_j^\dagger A_j$. Hence $\{\frac{c_j}{\sqrt{d_A}} A_j\}$ could be a set of Kraus operators for a quantum channel on system A , and $\{\frac{c_j}{\sqrt{d_B}} B_j\}$ could be a set of Kraus operators for a quantum channel on system B .

The unitary U can be implemented with some probability using the following protocol. Assume the input state is $|\Psi\rangle_{AB}$. Suppose there is a Schmidt-rank- r entangled resource state $|\psi\rangle = \frac{1}{\sqrt{r}} \sum_{j=1}^r |j\rangle_e |j\rangle_f$, where e and f are r -dimensional ancillary systems on the A and B side, respectively. The protocol also uses r -dimensional ancillary systems a and b on the A and B side, respectively. The a and b are initialized in the state $|0\rangle$.

1. Perform a local unitary on Aa that implements a quantum channel on A with $\frac{c_j}{\sqrt{d_A}} A_j$ as Kraus operators, so that the output of a in its computational basis contains full information about which Kraus operator was applied on A . (However, we do not perform a measurement on a at this stage.) Similarly, perform a local unitary on Bb , which implements a quantum channel on B with $\frac{c_j}{\sqrt{d_B}} B_j$ as Kraus operators.

2. Perform a local controlled-cyclic-shift gate on ae , and measure e in the computational basis. Similarly, perform a local controlled-cyclic-shift gate on bf , and measure f in the computational basis. Perform a Fourier gate on a and then measure a in the computational basis. Perform a different unitary on b with the first row

in its matrix proportional to $(1/c_1, \dots, 1/c_r)$, and then measure b in the computational basis.

In general, the protocol implements the nonlocal unitary U with probability $1/r^3$. However, when c_j are all equal, the above procedure implements the (possibly non-unitary) operator $V_m = \sum_{j=1}^r e^{2\pi i m j/r} A_j \otimes B_{1+(j+l-2) \bmod r}$ for $l, m \in \{1, \dots, r\}$, and l, m take their possible values with equal probabilities; hence, the success probability is $1/r^2$ in this case.

VI. TWO CONJECTURES

In this section we discuss two conjectures, respectively arising in the literature and this paper. The first conjecture is related to the dimension of reference systems of input states saturating the assisted entangling power. The second conjecture is to construct the upper bound of assisted entangling power in terms of the Schmidt rank of input bipartite unitaries. They both aim for a further understanding of the assisted entangling power.

A. The dimension of reference systems of assisted entangling power

If $|\psi\rangle_{AR_A:BR_B}$ maximizes the function $E(U(|\psi\rangle)) - E(|\psi\rangle)$ of (3), then we call it the assisted state of U , and the dimensions of R_A and R_B are respectively denoted as d_{R_A} and d_{R_B} . Let $R''_A = R_A R'_A$ and $R''_B = R_B R'_B$ be a bigger reference system and $|\varphi\rangle$ a pure state of the system $R'_A R'_B$. Then the state $|\psi\rangle \otimes |\varphi\rangle \in \mathcal{H}_{R''_A R''_B}$ is another assisted state of U . Hence, there are infinitely many assisted states, and the dimension of reference system can be arbitrarily large. On the other hand, it is an open problem to derive the minimum dimension of reference system, respectively denoted as $d_{R_A}^{opt}$ and $d_{R_B}^{opt}$. As the remarks in [2] suggest, it is an open problem to find $d_{R_A}^{opt}$ (or $d_{R_B}^{opt}$) as a function of d_A, d_B only, or as a function of U for generic U with a fixed pair of (d_A, d_B) . So far there is no evidence whether $d_{R_A}^{opt}$ is finite. To estimate the assisted entangling power, it was asked whether [44]

$$d_{R_A}^{opt} \leq d_A, \quad (41)$$

$$d_{R_B}^{opt} \leq d_B. \quad (42)$$

If U is a controlled unitary controlled from the A side, then $d_{R_B}^{opt}$ could be at most d_B by Proposition 19 (ii). It is a hint to the above conjecture. Since $d_A, d_B, d_{R_A}^{opt}$, and $d_{R_B}^{opt}$ are from the same pure state $|\psi\rangle$, we have $\text{sr}(\psi) \leq \min\{d_A d_{R_A}^{opt}, d_B d_{R_B}^{opt}\}$, where sr means the Schmidt rank. We do not know whether the two conjectured inequalities (41) and (42) are independent.

B. The upper bound of assisted entangling power

In Proposition 19, we have obtained an upper bound of assisted entangling power of bipartite controlled unitaries. We present a conjecture similar to Lemma 23.

Conjecture 27 *Let U be a bipartite unitary. We have*

$$\log_2 \text{Sch}(U) \geq K_{Ea}(U) \geq K_E(U), \quad (43)$$

and the two inequalities become equalities at the same time. When they are equalities, the input state can be chosen as a product state $|\Psi\rangle_{AR_A} \otimes |\Phi\rangle_{BR_B}$.

It would be a tighter upper bound than the first inequality in (37), because $\text{Sch}(U) \leq \min\{d_A^2, d_B^2\}$. Note that if the assisted entangling power is replaced with the entangling power, then the conjecture holds by definition. We provide a few evidences supporting the conjecture. The inequality holds for any two-qubit unitary U , whose Schmidt rank can be 1, 2, or 4 [2]. If $\text{Sch}(U) = 2$, then the inequality follows from Lemma 9. If $\text{Sch}(U) = 4$, then the inequality follows from Lemma 23. If $U = \sum_j P_j \otimes U_j$ is controlled with m terms, then Proposition 19 (i) implies that the inequality in (43) holds when the U_j are linearly independent. We prove a special case of (43). Suppose the assisted state of U on \mathcal{H}_{AB} can be written as

$$|\psi\rangle = \sqrt{a}|\mu\rangle_{AR_A:BR_B} + \sqrt{1-a}|\nu\rangle_{AR_A:BR_B}, \quad (44)$$

where $a \in [0, 1]$, and $|\mu\rangle, |\nu\rangle$ are orthogonal product states, and the R_B space of $|\mu\rangle$ is orthogonal to that of $|\nu\rangle$. Then

$$\begin{aligned} & K_{Ea}(U) \\ &= E(U|\psi\rangle) - E(|\psi\rangle) \\ &= S(\text{Tr}_{BR_B} U|\psi\rangle\langle\psi|U^\dagger) - S(\text{Tr}_{BR_B} |\psi\rangle\langle\psi|) \\ &= S(a\text{Tr}_{BR_B} U|\mu\rangle\langle\mu|U^\dagger + (1-a)\text{Tr}_{BR_B} U|\nu\rangle\langle\nu|U^\dagger) \\ &\quad - S(\text{Tr}_{BR_B} |\psi\rangle\langle\psi|) \\ &\leq aS(\text{Tr}_{BR_B} U|\mu\rangle\langle\mu|U^\dagger) + (1-a)S(\text{Tr}_{BR_B} U|\nu\rangle\langle\nu|U^\dagger) \\ &\quad + H(a, 1-a) - S(\text{Tr}_{BR_B} |\psi\rangle\langle\psi|) \\ &\leq aS(\text{Tr}_{BR_B} U|\mu\rangle\langle\mu|U^\dagger) + (1-a)S(\text{Tr}_{BR_B} U|\nu\rangle\langle\nu|U^\dagger) \\ &\leq \log_2 \text{Sch}(U). \end{aligned} \quad (45)$$

The first inequality follows from Lemma 1 (ii). The second inequality follows from Lemma 2 because the vector $\text{des}(a, 1-a)$ is majorized by the Schmidt vector of $|\psi\rangle$ by [33, Corollary 4]. The last inequality follows from the fact that $|\mu\rangle, |\nu\rangle$ are both product states.

If the R_B space of $|\mu\rangle$ is not orthogonal to that of $|\nu\rangle$, then we construct another pure state

$$|\varphi\rangle = \sqrt{a}|\mu\rangle_{AR_A:BR_B} - \sqrt{1-a}|\nu\rangle_{AR_A:BR_B}. \quad (46)$$

Then

$$\begin{aligned}
& \min_{x=U|\psi\rangle, U|\varphi\rangle} E(x) \\
& \leq \frac{1}{2}E(U|\psi\rangle) + \frac{1}{2}E(U|\varphi\rangle) \\
& \leq S\left(\frac{1}{2}\text{Tr}_{BR_B} U|\psi\rangle\langle\psi|U^\dagger + \frac{1}{2}\text{Tr}_{BR_B} U|\varphi\rangle\langle\varphi|U^\dagger\right) \\
& = S(a\text{Tr}_{BR_B} U|\mu\rangle\langle\mu|U^\dagger + (1-a)\text{Tr}_{BR_B} U|\nu\rangle\langle\nu|U^\dagger) \\
& \leq aS(\text{Tr}_{BR_B} U|\psi\rangle\langle\psi|U^\dagger) + (1-a)S(\text{Tr}_{BR_B} U|\varphi\rangle\langle\varphi|U^\dagger) \\
& \quad + H(a, 1-a) \\
& \leq \log_2 \text{Sch}(U) + E(\psi). \tag{47}
\end{aligned}$$

The inequalities hold by arguments similar to that for (45). Since $E(\psi) = E(\varphi)$, we have

$$\begin{aligned}
& \min\{E(U|\psi) - E(|\psi\rangle), E(U|\varphi) - E(|\varphi\rangle)\} \\
& \leq \log_2 \text{Sch}(U). \tag{48}
\end{aligned}$$

However we do not know whether the inequality holds when the minimum is replaced with the maximum.

VII. CONCLUSIONS

In this paper we have analytically derived the entangling power of Schmidt-rank-two bipartite unitary, Schmidt-rank-three permutation unitary and some special non-controlled unitary operations. In particular the entangling power of any bipartite permutation unitary of Schmidt rank three can only take one of two values: $\log_2 9 - 16/9$ or $\log_2 3$ ebits. We have proposed the upper bound of the assisted entangling power of bipartite controlled unitaries, and the necessary and sufficient conditions for this upper bound. The entangling power, assisted entangling power and disentangling power of $2 \times d_B$ permutation unitaries of Schmidt rank four are all 2 ebits. These quantities are also derived for generalized Clifford operators. We further show that any bipartite permutation unitary of Schmidt rank greater than two has entangling power greater than 1.223 ebits.

We also have constructed GCNOT gates, which is a parameterized Schmidt-rank-two bipartite unitary whose assisted entangling power is 1 ebit. It generalizes the known CNOT gate for two-qubit systems. Further we have constructed the inequalities between entangling power and assisted entangling power, and conditions by which the inequalities hold. We also have shown the connection to the disentangling power by proposing a probabilistic protocol for implementing bipartite unitaries. The next step is to analyze the conjectures in Sec. VI. By studying the properties of the different types of entangling power, we hope to get more insight into the question of whether there is a bipartite unitary such that its entanglement cost is strictly greater than its assisted entangling power.

Acknowledgments

L.C. was supported by the NSF of China (Grant No. 11501024), and the Fundamental Research Funds for the Central Universities (Grants No. 30426401 and No. 30458601). L.Y. was supported by NICT-A (Japan).

Appendix A: The proof of Lemma 8

Proof. We prove the assertions when all P_j have rank one. One can similarly prove the assertions.

(i) Let $|\alpha, \beta\rangle$ be the critical state of U , where $|\alpha\rangle = \sum_j \sqrt{p_j} |j, a_j\rangle_{AR_A}$, $\sum_j p_j = 1$, and $p_j > 0$. Hence,

$$\begin{aligned}
K_E(U) &= E\left(\sum_j \sqrt{p_j} |j, a_j\rangle_{AR_A} \otimes (U_j)_B |\beta\rangle_{BR_B}\right) \\
&= E\left(\sum_j \sqrt{p_j} |j\rangle_A \otimes (U_j)_B |\beta\rangle_{BR_B}\right) \\
&= E\left(U \sum_j \sqrt{p_j} |j\rangle_A \otimes |\beta\rangle_{BR_B}\right) \\
&\leq \max_{|\alpha\rangle \in \mathcal{H}_A, |\beta\rangle \in \mathcal{H}_{BR_B}} E(U(|\alpha\rangle|\beta\rangle)) \\
&\leq K_E(U). \tag{A1}
\end{aligned}$$

The second equality follows from the fact that local unitaries does not change the amount of entanglement. Hence, the first equality in (12) follows. In particular, $\sum_j \sqrt{p_j} |j\rangle_A \otimes |\beta\rangle_{BR_B}$ is another critical state of U .

The second equality in (12) follows from the definition of E and the assumption $|\alpha\rangle = \sum_{j=1}^{d_A} \sqrt{p_j} |j\rangle$, where $p_j \geq 0$, $\sum_{j=1}^{d_A} p_j = 1$. To prove the inequalities in (12), we note that $K_E(U) \leq \log_2 \text{Sch}(U)$ is the definition of K_E . The last inequality of (12) follows from the definition of U . The last assertion of (i) holds because $U(|\alpha, \beta\rangle)$ has Schmidt rank at most $\text{Sch}(U)$.

(ii) The proof is similar to that of (i). In particular, the first equality in (13) follows by applying (12) to both systems of U .

(iii) Equation (14) is trivial. An example for which the inequality holds is $U = \sum_{j=0}^3 |j\rangle\langle j| \otimes \sigma_j$. The entangling power with a one-qubit ancilla R_B initially maximally entangled with B is 2 ebits, while the entangling power without R_B is 1 ebit.

On the other hand, an example for which the inequality does not hold is $U = \sum_{j=1}^{d_A} |j\rangle\langle j| \otimes V_j$, where $d_A \leq d_B$, V_j are $d_B \times d_B$ permutation matrices whose $(j, 1)$ element is 1, and at the same time they do not have simultaneous singular value decomposition. One can easily verify that such V_j exist. So U is not locally equivalent to a controlled unitary from the B side. Evidently, U has Schmidt rank d_A , and thus $K_E(U) \leq \log_2 d_A$. This upper bound is achievable, and a critical state of U is the input state $(\frac{1}{\sqrt{d_A}} \sum_{j=1}^{d_A} |j\rangle_A) \otimes |1\rangle_B$. Using these results,

(12) and (14) we have

$$\begin{aligned}
\log_2 d_A &\geq K_E(U) \\
&= \max_{|\alpha\rangle \in \mathcal{H}_A, |\beta\rangle \in \mathcal{H}_{BR_B}} E(U(|\alpha\rangle|\beta\rangle)) \\
&\geq \max_{|\alpha\rangle \in \mathcal{H}_A, |\beta\rangle \in \mathcal{H}_B} E(U(|\alpha\rangle|\beta\rangle)) \\
&= \log_2 d_A.
\end{aligned} \tag{A2}$$

Hence the equality in (14) holds.

(iv) The assertion follows from (A1) and (13). This completes the proof. \square

Appendix B: The proof of Lemma 12

Proof. Since U is unitary, V_1 and V_3 are also unitary matrices. So U is a controlled unitary controlled from both A and B sides. Applying Lemma 8 to (20), we have

$$\begin{aligned}
K_E(U) &= \max_{p_j \geq 0, \sum_{j=1}^3 p_j = 1, |\beta\rangle \in \mathcal{H}_B} \\
&\quad S(p_1|\beta\rangle\langle\beta| + p_2|\beta_1\rangle\langle\beta_1| + p_3|\beta_2\rangle\langle\beta_2|), \tag{B1}
\end{aligned}$$

where $|\beta_1\rangle = (I_m \oplus I_n \oplus V_1)|\beta\rangle$ and $|\beta_2\rangle = (I_m \oplus V_3 \oplus I_p)|\beta\rangle$. There is a unitary $W = W_1 \oplus W_2 \oplus W_3$, such that

$$\begin{aligned}
W|\beta\rangle &= (a, 0, \dots, 0, b, 0, 0, \dots, 0, c, 0, 0, \dots, 0), \\
W|\beta_1\rangle &= (a, 0, \dots, 0, b, 0, 0, \dots, 0, c_1, c_2, 0, \dots, 0), \\
W|\beta_2\rangle &= (a, 0, \dots, 0, b_1, b_2, 0, \dots, 0, c, 0, 0, \dots, 0),
\end{aligned} \tag{B2}$$

where $|b_1|^2 + |b_2|^2 = |b|^2$ and $|c_1|^2 + |c_2|^2 = |c|^2$. Let $X = I_m \oplus X_1 \oplus I_{n-2} \oplus X_2 \oplus I_{q-2}$ be a unitary operator with 2×2 unitary matrices X_1, X_2 . We can find an X such that the first entry of $X_1(b_1, b_2)^T$ is the same as that of $X_1(b, 0)^T$, and the first entry of $X_2(c_1, c_2)^T$ is the same as that of $X_2(c, 0)^T$. Now we can find a suitable unitary Y such that each of the three states $YXW|\beta\rangle$, $YXW|\beta_1\rangle$, and $YXW|\beta_2\rangle$ contains exactly three nonzero entries. They are in the same rows of the three states. Let $|\beta'\rangle$, $|\beta'_1\rangle$ and $|\beta'_2\rangle$ be qutrits which respectively consist of the three nonzero entries. We may assume $|\beta'\rangle = (a, b', c')^T$, $|\beta'_1\rangle = (a, b', c'e^{i\alpha})^T$, and $|\beta'_2\rangle = (a, b'e^{i\beta}, c')^T$. Since the von Neumann entropy is invariant up to unitary transformation, (B1) implies that

$$\begin{aligned}
K_E(U) &= \max_{p_j \geq 0, \sum_{j=1}^3 p_j = 1, |a|^2 + |b'|^2 + |c'|^2 = 1, c \geq 0} \\
&\quad S(\rho), \tag{B3}
\end{aligned}$$

where the state $\rho = p_1|\beta'\rangle\langle\beta'| + p_2|\beta'_1\rangle\langle\beta'_1| + p_3|\beta'_2\rangle\langle\beta'_2|$. By computation we have $\det \rho = p_1 p_2 p_3 |ab'c'(1 - e^{i\alpha})(1 - e^{i\beta})|^2$. It follows from the restriction in (B3) that $\det \rho \leq \frac{16}{729}$. Hence,

$$K_E(U) \leq \max_{\sigma \geq 0, \text{Tr} \sigma = 1, \text{rank} \sigma \leq 3, \det \sigma \leq \frac{16}{729}} S(\sigma). \tag{B4}$$

Let the three eigenvalues of σ be λ_1, λ_2 and λ_3 in the ascending order. Since $\det \sigma \leq \frac{16}{729}$, the eigenvalues cannot be all equal. That is, we have either $\lambda_1 < \lambda_2$ or $\lambda_2 < \lambda_3$.

Assume that the maximum of (B4) is achieved when $\det \sigma < \frac{16}{729}$. If $\lambda_1 < \lambda_2$, then we can find a small $\epsilon > 0$ to construct a quantum state σ' of three eigenvalues $\lambda_1 + \epsilon$, $\lambda_2 - \epsilon$, and λ_3 still in the ascending order, and at the same time $\det \sigma' \leq \frac{16}{729}$. Since $\sigma' \prec_s \sigma$, it follows from Lemma 2 that $S(\sigma') > S(\sigma)$. It gives us a contradiction with the assumption. One may similarly find the contradiction when $\lambda_2 < \lambda_3$. So the maximum of (B4) is achievable when $\det \sigma = \frac{16}{729}$. Since $\det \sigma = \lambda_1 \lambda_2 \lambda_3$ and $\sum_{j=1}^3 \lambda_j = 1$, using the inequality $\lambda_2 + \lambda_3 \geq 2\sqrt{\lambda_2 \lambda_3}$ we obtain

$$1 - \lambda_1 \geq \frac{8}{27\sqrt{\lambda_1}}. \tag{B5}$$

The inequality holds only if $\lambda_1 \geq 1/9$. Using the upper bound $\lambda_1 \leq 1/3$, one can plot $S(\sigma)$ as the function of λ_1 and show that the maximum is achievable when $\lambda_1 = 1/9$, $\lambda_2 = \lambda_3 = 4/9$. It follows from (B4) that $K_E(U) \leq \log_2 9 - 16/9$. The equality holds for the permutation unitaries that fit into the form (20), as shown in the proof of [6, Proposition 1]. This completes the proof. \square

Appendix C: The proof of Proposition 15

Proof. Since U has Schmidt rank three we have $n \in [1, d_B - 2]$. Suppose the input state is $|\alpha, \beta\rangle_{AR_A, BR_B} = \sum_{j=1}^2 a_j |j, \alpha_j\rangle_{AR_A} \otimes \sum_{k=1}^{d_B} b_k |k, \beta_k\rangle_{BR_B}$. The entangling power of U is equal to the maximum amount of entanglement contained in the state

$$\begin{aligned}
&U|\alpha, \beta\rangle_{AR_A, BR_B} \\
&= \sqrt{x} \sum_{j=1}^2 a_j |j, \alpha_j\rangle_{AR_A} \sum_{k=1}^n c_k |k, \beta_k\rangle_{BR_B} \\
&\quad + a_2 \sqrt{1-x} |1, \alpha_2\rangle_{AR_A} \sum_{k=n+1}^{d_B} c_k |k, \beta_k\rangle_{BR_B} \\
&\quad + a_1 \sqrt{1-x} |2, \alpha_1\rangle_{AR_A} \sum_{k=n+1}^{d_B} c_k |k, \beta_k\rangle_{BR_B} \\
&:= \sqrt{x} |\psi_1\rangle + a_2 \sqrt{1-x} |\psi_2\rangle + a_1 \sqrt{1-x} |\psi_3\rangle, \tag{C1}
\end{aligned}$$

where the parameters $x = \sum_{k=1}^n |b_k|^2$, and $c_k = \frac{b_k}{\sqrt{x}}$ for $k \leq n$, and $c_k = \frac{b_k}{\sqrt{1-x}}$ for $k > n$. Besides, the three product states $|\psi_1\rangle, |\psi_2\rangle$, and $|\psi_3\rangle$ are pairwise orthogo-

nal. We have

$$\begin{aligned}
K_E(U) &= \max_{x, a_j, \alpha_j, c_k, \beta_k} S \left(x \text{Tr}_{BR_B} |\psi_1\rangle\langle\psi_1| + \right. \\
&\quad \left. (1-x) \text{Tr}_{BR_B} (a_2 |\psi_2\rangle + a_1 |\psi_3\rangle) (a_2^* \langle\psi_2| + a_1^* \langle\psi_3|) \right) \\
&\leq \max_{x, a_j, \alpha_j, c_k, \beta_k} [H(x, 1-x) + \\
&\quad (1-x) S \left(\text{Tr}_{BR_B} (a_2 |\psi_2\rangle + a_1 |\psi_3\rangle) (a_2^* \langle\psi_2| + a_1^* \langle\psi_3|) \right)] \\
&= \max_{x, a_j, c_k, \beta_k} [H(x, 1-x) + \\
&\quad (1-x) S \left(\text{Tr}_{AR_A} (|a_2|^2 |\psi_2\rangle\langle\psi_2| + |a_1|^2 |\psi_3\rangle\langle\psi_3|) \right)]. \tag{C2}
\end{aligned}$$

The inequality follows from Lemma 1, and the last equality follows from C1. The inequality becomes the equality when $|\alpha_1\rangle$ and $|\alpha_2\rangle$ are orthogonal. This is achievable, because $|\alpha_1\rangle$ and $|\alpha_2\rangle$ do not appear in the von Neumann entropy of the final equation of (C2). The entropy is upper bounded by the entangling power of $V = |1\rangle\langle 2| \otimes I_B + |2\rangle\langle 1| \otimes C$, which can be obtained using the paragraph above Proposition 10. Let the entangling power of V be a positive constant $M \leq 1$. Thus, $K_E(U) \leq H(x, 1-x) + (1-x)M$. It is maximized at $x = \frac{1}{e^M + 1}$ by considering the behavior of its first derivative in the whole range $(0, 1)$. We have thus obtained the assertion. This completes the proof. \square

Appendix D: The proof of Proposition 18

Proof. Assume that the claim holds for any (and all) bipartite permutation unitary which is not BCPU from the A side. (The definition of BCPU is just above Lemma 7.) We assert that under such assumption, the claim holds for any U which is a BCPU from the A side, say $U = (\oplus_j)_A V_j$, where the $d_j \times d_B$ bipartite unitary V_j is not a BCPU from the A side, and $\sum_j d_j = d_A$. If one of the V_j 's has Schmidt rank greater than two, then the assertion follows from Lemma 7 and the assumption. So any V_j has Schmidt rank of at most two, and it is a controlled unitary [7]. If the A -direct sum of some V_j 's has Schmidt rank three then the assertion follows from Lemma 7 and Proposition 13. So it suffices to consider the case that k terms of V_j 's ($k \geq 2$) each have Schmidt rank one or two and their A -direct sum has Schmidt rank four. Suppose k is the minimum integer such that the previous sentence holds. Suppose $k \geq 3$; then under the condition established above that the A -direct sum of any set of V_j 's has Schmidt rank not equal to three, it must be that any $k-1$ terms in the k terms satisfy that their A -direct sum has Schmidt rank two, and we may view these terms as one V_j in the argument below. Then it suffices to prove the assertion when $k = 2$, i.e., when $U = V_1 \oplus_A V_2$ has Schmidt rank four, where V_1 and V_2 are of Schmidt

rank two. From [6, Lemma 15(i)], any bipartite permutation unitary of Schmidt rank two is equivalent under local permutation unitaries to a controlled-permutation unitary with two terms, where the direction of control may be from either side. If one of V_1 and V_2 is controlled from the A side with two terms, then the assertion follows again from Lemma 7 and Proposition 13.

So we may assume $V_j = W_j \otimes P_j + X_j \otimes Q_j$ for $j = 1, 2$, where W_j and X_j are the direct sum of a permutation matrix of order d_j with a zero matrix of order d_{3-j} , and P_j and Q_j are two partial permutation matrices of order d_B such that $P_j + Q_j$ is a permutation matrix. From $U = V_1 \oplus_A V_2$, there is no common nonzero row or column for the pair of matrices W_1 and W_2 , and the same holds for the pairs of matrices (W_1, X_2) , (X_1, W_2) , and (X_1, X_2) . Since $U = V_1 \oplus_A V_2$ has Schmidt rank four, the four matrices P_1, P_2, Q_1, Q_2 are linearly independent. We can find a Schmidt-rank-two uniformly entangled state $|\alpha\rangle_{AR_A}$ such that the four states $(Y_j \otimes I_{R_A})|\alpha\rangle_{AR_A}$ are pairwise orthogonal, where $Y_j = W_1, X_1, W_2$, and X_2 ; a type of choice of such state is given by $\frac{1}{\sqrt{2}}(|j\rangle_A \otimes |1\rangle_{R_A} + |k\rangle_A \otimes |2\rangle_{R_A})$, where $|j\rangle_A$ and $|k\rangle_A$ are computational basis states, and $W_1|j\rangle_A$ and $X_1|j\rangle_A$ are nonzero and orthogonal to each other, and $W_2|k\rangle_A$ and $X_2|k\rangle_A$ are nonzero and orthogonal to each other, and $W_2|j\rangle_A = X_2|j\rangle_A = W_1|k\rangle_A = X_1|k\rangle_A = 0$. We can also find another Schmidt-rank-two uniformly entangled state $|\beta\rangle_{BR_B}$ such that three of the four states $(Z_j \otimes I_{R_B})|\beta\rangle_{BR_B}$ are pairwise orthogonal where $Z_j = P_1, Q_1, P_2$, and Q_2 . The fourth state is either the same as one of the three states, or orthogonal to all of them. Let $|\alpha\rangle_{AR_A} \otimes |\beta\rangle_{BR_B}$ be the input state; then the corresponding amount of output entanglement is either 2 ebits or $-\frac{2}{3} \log_2 \frac{2}{3} - 2 \times \frac{1}{6} \log_2 \frac{1}{6} = \log_2 3 - \frac{1}{3} > 1.251$ ebits. So the assertion holds. From now on we assume that U is not a BCPU. If U is of Schmidt rank three, the claim already follows from Proposition 13. Thus, in the following we assume U is of Schmidt rank at least four.

Suppose U contains at least three nonzero blocks in one big column. We may assume that the big column is the first big column in U , and its first three blocks are nonzero. Up to local permutations on B we may assume that the j 'th column of the j 'th block is nonzero for $j = 1, 2, 3$. Let the initial state on AR_A be a product state $|1\rangle_A |1\rangle_{R_A}$, and let the initial state on BR_B be $|\phi\rangle_{BR_B} = \frac{1}{\sqrt{3}} \sum_{j=1}^3 |j\rangle_B |j\rangle_{R_B}$. We obtain that the output entanglement is exactly $\log_2 3$ ebits and the assertion holds.

Hence, $U = \sum_{j,k=1}^{d_A} |j\rangle\langle k| \otimes U_{jk}$ has exactly two nonzero blocks in every big column. We consider the four blocks that are the intersections of two big rows and two big columns in U . Denote V as the submatrix formed by these four blocks. We have $V = \sum_{j,k=1}^2 |j\rangle\langle k| \otimes U_{jk}$, where each U_{jk} is a $d_B \times d_B$ partial permutation matrix.

Suppose there is a V such that all four blocks in it are nonzero. Since each big column of V contains the only nonzero blocks in the corresponding big column of U , all columns of V are nonzero. Thus, V contains $2d_B$

nonzero elements; hence, all rows of V are nonzero, and V is a permutation matrix. Since U is not a BCPU, we obtain $U = V$. Then since we assumed previously that U is of Schmidt rank at least four, the Schmidt rank of U is exactly four. The assertion follows from Proposition 17.

It remains to consider the case that any V contains at most three nonzero blocks. The above assumptions imply that there is a V containing exactly three nonzero blocks. Assume that any V has Schmidt rank smaller than three. Then up to local permutation matrices we may assume that $U_{11} = I_r \oplus 0_{d_B-r}$ and $U_{12} = U_{21} = 0_r \oplus P$, where $r \in [1, d_B - 1]$ and P is a permutation matrix. Up to local permutation unitaries we may assume $U_{23} \neq 0$ and $U_{32} \neq 0$. Applying the above assumption about V to the four blocks $U_{11}, U_{12}, U_{31}, U_{32}$, we get that $U_{32} = U_{11}$. Similarly, $U_{23} = U_{11}$. Up to local permutation unitaries we may assume $U_{34} \neq 0$ and $U_{43} \neq 0$. Applying the above assumption about V to the four blocks $U_{12}, U_{14}, U_{32}, U_{34}$, we have $U_{34} = U_{12}$. Similarly, $U_{43} = U_{12}$. Continuing in this vein, and noting that U is not a BCPU, we get that U has Schmidt rank two. It is a contradiction and thus there exists a V of Schmidt rank three.

Up to local permutation matrices, the three nonzero blocks of V are $U_{11} = I_r \oplus 0_{d_B-r}$, U_{12} , and U_{21} . Up to local permutations on \mathcal{H}_A we may assume that U_{23} is the other nonzero block in the second big column of U . The first r rows of U_{12} are zero, and the first r columns of U_{21} are zero. Since V is of Schmidt rank three, we can find four integers s, t, u, v , such that $s > r$ and $v > r$, and $|1\rangle\langle 1|$, $|s\rangle\langle t|$, and $|u\rangle\langle v|$ are pairwise different entries and respectively belong to U_{11} , U_{12} , and U_{21} . We choose a nonnormalized input state $|\psi\rangle = (|11\rangle + |22\rangle)_{AR_A} \otimes [|11\rangle + (1-\delta_{1,t})(1-\delta_{v,t})|tt\rangle + |vv\rangle]_{BR_B}$. The corresponding output state is $U|\psi\rangle = \frac{1}{2}|11\rangle_{AR_A} \otimes |b_1\rangle_{BR_B} + \frac{1}{2}|12\rangle_{AR_A} \otimes |b_2\rangle_{BR_B} + \frac{1}{2}|21\rangle_{AR_A} \otimes |b_3\rangle_{BR_B} + \frac{1}{2}|32\rangle_{AR_A} \otimes |b_4\rangle_{BR_B}$.

In the cases $t = 1$ or $v = t$, we have $\langle b_1|b_2\rangle = \langle b_1|b_3\rangle = \langle b_2|b_3\rangle = 0$, and $|b_4\rangle$ may be equal to $|b_1\rangle$ or $|b_3\rangle$, or orthogonal to all of $|b_1\rangle$, $|b_2\rangle$, and $|b_3\rangle$. Thus, the entanglement of the output state is 2 ebits or $-2 \times \frac{1}{4} \log_2 \frac{1}{4} - \frac{1}{2} \log_2 \frac{1}{2} = 1.5$ ebits.

The remaining case is that $t, v, 1$ are three distinct integers. Since U is a permutation matrix, we have $\langle b_1|b_2\rangle = \langle b_1|b_3\rangle = \langle b_2|b_4\rangle = 0$, but $\langle b_2|b_3\rangle$ may be 0 or $\frac{1}{\sqrt{2}}$, since we may always choose the integers s, t, u, v such that $\langle b_2|b_3\rangle \neq 1$, and we indeed make such choices here to maximize the output entanglement. An example for the case $\langle b_2|b_3\rangle = \frac{1}{\sqrt{2}}$ is given by $r = 1$, $U_{12} = 0_1 \oplus 1_1 \oplus 0_1$, and $U_{21} = 0_1 \oplus 1_2$, where x_k is x times the identity matrix of order k ; in such case $t = 2$ and $v = 3$. The case that $\langle b_2|b_3\rangle = 0$ would give rise to an output entanglement which is too large, thus, in the following we assume $\langle b_2|b_3\rangle = \frac{1}{\sqrt{2}}$. Under such condition, it is not hard to show that $\langle b_1|b_4\rangle$ and $\langle b_3|b_4\rangle$ may be 0, $\frac{1}{2}$, $\frac{1}{\sqrt{2}}$, or 1.

Since U_{11} and U_{21} are partial permutation matrices and do not have a common nonzero column, if one of the two quantities $\langle b_1|b_4\rangle$ and $\langle b_3|b_4\rangle$ is equal to 1, the

other must be 0. Among the possible cases, the case with the smallest entanglement of the output state is when $\langle b_2|b_3\rangle = \frac{1}{\sqrt{2}}$, and one of $\langle b_1|b_4\rangle$ and $\langle b_3|b_4\rangle$ is 1 (and the other is 0). The entanglement of the output state is $H(\frac{1}{4}, \frac{3+\sqrt{5}}{8}, \frac{3-\sqrt{5}}{8}) > 1.223$ ebits in this case, where $H(\{x_1, \dots, x_n\}) := -\sum_{j=1}^n x_j \log_2 x_j$ is the entropy function.

In summary, $K_E(U) > 1.223$ ebits and the claim holds. \square

Appendix E: The proof of Proposition 19

Proof. (i) The last inequality in (25) is obtained by the definition of $K_{Ea}(U)$ and $K_E(U)$. Let us prove the equality in (25). Let $\rho_{AR_A BR_B} = |\psi\rangle\langle\psi|_{AR_A BR_B}$. We have

$$\begin{aligned} & E(U(|\psi\rangle)) - E(|\psi\rangle) \\ &= S\left[\text{Tr}_{AR_A}\left(\left(\sum_{j=1}^m P_j \otimes U_j\right)_{AB}(\rho_{AR_A BR_B})\right.\right. \\ &\quad \left.\left.\left(\sum_{k=1}^m P_k \otimes U_k^\dagger\right)_{AB}\right)\right] - S(\rho_{BR_B}) \\ &= S\left(\sum_{j=1}^m U_j M_j U_j^\dagger\right) - S(\rho_{BR_B}), \end{aligned} \quad (\text{E1})$$

where $M_j = \text{Tr}_{AR_A}\left((P_j)_{A\rho_{AR_A BR_B}}\right)$, $\forall j$. Hence $\sum_j M_j = \rho_{BR_B}$ and each M_j is a positive semidefinite matrix. Since ρ_{BR_B} is arbitrary, we obtain the equality in (25) by the definition of $K_{Ea}(U)$.

It remains to prove the first inequality in (25). We present two different proofs. The first is simpler but the second proof is useful in the proof of (ii) below. The first proof is that the controlled unitaries with m terms can be implemented using a simple protocol in [13] using a maximally entangled state of Schmidt rank m , which contains $\log_2 m$ ebits; thus, $E_c(U) \leq \log_2 m$, and from (5) we obtain $K_{Ea}(U) \leq \log_2 m$. The second proof is as follows. We use the quantity in the third line of (25) in place of $K_{Ea}(U)$. Let $M'_j = U_j M_j U_j^\dagger$ for $j = 1, \dots, m$. We have

$$\begin{aligned} & S\left(\sum_j U_j M_j U_j^\dagger\right) - S(\rho) \\ &\leq S\left(\sum_j M'_j\right) - \sum_j \text{Tr} M'_j \cdot S\left(\frac{M'_j}{\text{Tr} M'_j}\right) \\ &= S\left(\sum_j \text{Tr} M'_j \frac{M'_j}{\text{Tr} M'_j}\right) - \sum_j \text{Tr} M'_j \cdot S\left(\frac{M'_j}{\text{Tr} M'_j}\right) \\ &\leq H(\{\text{Tr} M'_j\}). \end{aligned} \quad (\text{E2})$$

The first inequality follows from the concavity of von Neumann entropy and $\rho = \sum_j M_j = \sum_j \text{Tr} M_j \cdot \frac{M_j}{\text{Tr} M_j}$.

The equality in (E2) holds because the von Neumann entropy is invariant under unitary operations. The second inequality in (E2) follows from the first inequality in (11), and the observation that $\{\text{Tr} M'_j\}$ is a probability distribution. Since $j = 1, \dots, m$, we have $H(\{\text{Tr} M'_j\}) \leq \log_2 m$ and the first inequality in (25) holds.

(ii) Suppose the first inequality in (25) becomes the equality. It is equivalent to the condition that both inequalities in (E2) become equalities, and $H(\{\text{Tr} M'_j\}) = \log_2 m$. It implies that any M'_j is nonzero. Lemma 1 implies that $M_j \propto \rho$ for any j , and $M'_j M'_k = 0$ for $j \neq k$. Since $H(\{\text{Tr} M'_j\}) = \log_2 m$ and $M'_j = U_j M_j U_j^\dagger$, we have $M_j = \frac{1}{m} \rho$. Thus,

$$\rho(U_j^\dagger U_k \otimes I_{R_B}) \rho = 0 \quad (\text{E3})$$

for any j, k and $j \neq k$. Since ρ is a mixed state, we can project it onto a pure state in the Schmidt decomposition, namely $|\psi\rangle = \sum_i \sqrt{c_i} |a_i, b_i\rangle$. Then (E3) becomes $\sum_i c_i \langle a_i | U_j^\dagger U_k | a_i \rangle = 0$. Setting $\sigma = \sum_i c_i |a_i\rangle \langle a_i|$ implies the “only if” part except that $j < k$ is also allowed. It

can be excluded because $\text{Tr}(\sigma U_j^\dagger U_k) = 0$ is equivalent to $\text{Tr}(\sigma U_k^\dagger U_j) = 0$. On the other hand the “if” part follows by assuming $M_j = \frac{1}{m} \rho$ for $j = 1, \dots, m$.

To prove the last-but-one assertion, if U_i are all diagonal then so are $U_j^\dagger U_k$. Since $\text{Tr}(\sigma U_j^\dagger U_k) = 0$ for all $j \neq k$, we have $\text{Tr}(\sigma' U_j^\dagger U_k) = 0$ for all $j \neq k$, where σ' is the diagonal matrix whose diagonal entries are the same as those of σ . So σ' is still a quantum state.

To prove the last assertion, if U_i are all real, then $\text{Tr}(\sigma^* U_j^\dagger U_k) = 0$ for all $j \neq k$. The sum of this equation and $\text{Tr}(\sigma U_j^\dagger U_k) = 0$ implies $\text{Tr}(\sigma' U_j^\dagger U_k) = 0$ where $\sigma' = \frac{\sigma + \sigma^*}{2}$ is real.

(iii) The last claim follows from the first claim. If $K_E(U) = \log_2 m$, then $K_{Ea}(U) = \log_2 m$ by (i). It suffices to prove the statement that $K_{Ea}(U) = \log_2 m$ implies $K_E(U) = \log_2 m$. The statement follows from (ii) and Lemma 8 (i).

(iv) The statement follows from assertion (i) and Lemma 8 (i). This completes the proof. \square

-
- [1] H. Zhu, M. Hayashi, and L. Chen, Phys. Rev. Lett. **116**, 070403 (2016), URL <http://link.aps.org/doi/10.1103/PhysRevLett.116.070403>.
- [2] M. A. Nielsen, C. M. Dawson, J. L. Dodd, A. Gilchrist, D. Mortimer, T. J. Osborne, M. J. Bremner, A. W. Harrow, and A. Hines, Phys. Rev. A **67**, 052301 (2003), URL <http://link.aps.org/doi/10.1103/PhysRevA.67.052301>.
- [3] N. Linden, J. A. Smolin, and A. Winter, Phys. Rev. Lett. **103**, 030501 (2009), URL <http://link.aps.org/doi/10.1103/PhysRevLett.103.030501>.
- [4] M. Musz, M. Kus, and K. Zyczkowski, Phys. Rev. A **87**, 022111 (2013).
- [5] L. Chen and L. Yu, Phys. Rev. A **91**, 032308 (2015), URL <http://link.aps.org/doi/10.1103/PhysRevA.91.032308>.
- [6] L. Chen and L. Yu, Phys. Rev. A **93**, 042331 (2016), URL <http://link.aps.org/doi/10.1103/PhysRevA.93.042331>.
- [7] S. M. Cohen and L. Yu, Phys. Rev. A **87**, 022329 (2013), URL <http://link.aps.org/doi/10.1103/PhysRevA.87.022329>.
- [8] A. Soeda and M. Murao, New Journal of Physics **12**, 093013 (2010), URL <http://stacks.iop.org/1367-2630/12/i=9/a=093013>.
- [9] P. Zanardi, C. Zalka, and L. Faoro, Phys. Rev. A **62**, 030301 (R) (2000), URL <http://link.aps.org/doi/10.1103/PhysRevA.62.030301>.
- [10] L. Clarisse, S. Ghosh, S. Severini, and A. Sudbery, Phys. Rev. A **72**, 012314 (2005), URL <http://link.aps.org/doi/10.1103/PhysRevA.72.012314>.
- [11] L. Chen and L. Yu, Phys. Rev. A **89**, 062326 (2014), URL <http://link.aps.org/doi/10.1103/PhysRevA.89.062326>.
- [12] L. Chen and L. Yu, Annals of Physics **351**, 682 (2014), ISSN 0003-4916, URL <http://www.sciencedirect.com/science/article/pii/S0003491614002863>.
- [13] L. Yu, R. B. Griffiths, and S. M. Cohen, Phys. Rev. A **81**, 062315 (2010), URL <http://link.aps.org/doi/10.1103/PhysRevA.81.062315>.
- [14] D. Gottesman, PhD Thesis, Caltech (1997).
- [15] G. Smith and J. Yard, Science **321**, 1812 (2008), URL <http://www.sciencemag.org/content/321/5897/1812.full.pdf>, URL <http://www.sciencemag.org/content/321/5897/1812.abstract>.
- [16] K. Li, A. Winter, X. B. Zou, and G. C. Guo, Phys. Rev. Lett. **103**, 120501 (2009), URL <http://link.aps.org/doi/10.1103/PhysRevLett.103.120501>.
- [17] M. S. Leifer, L. Henderson, and N. Linden, Phys. Rev. A **67**, 012306 (2003), URL <http://link.aps.org/doi/10.1103/PhysRevA.67.012306>.
- [18] W. Dür, G. Vidal, J. I. Cirac, N. Linden, and S. Popescu, Phys. Rev. Lett. **87**, 137901 (2001), URL <http://link.aps.org/doi/10.1103/PhysRevLett.87.137901>.
- [19] J. Tyson, J. Phys. A: Math. Gen. **36**, 10101 (2003).
- [20] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, 2000).
- [21] R. F. Werner, Journal of Physics A: Mathematical and General **34**, 7081 (2001), URL <http://stacks.iop.org/0305-4470/34/i=35/a=332>.
- [22] C. King, Journal of Mathematical Physics **43**, 4641 (2002), URL <http://scitation.aip.org/content/aip/journal/jmp/43/10/10.1063/jmp.43.10.4641>.
- [23] N. Datta and M. B. Ruskai, Journal of Physics A: Mathematical and General **38**, 9785 (2005), URL <http://stacks.iop.org/0305-4470/38/i=45/a=005>.
- [24] C. Mendl and M. Wolf, Communications in Mathematical Physics **289**, 1057 (2009), ISSN 0010-3616, URL <http://dx.doi.org/10.1007/s00220-009-0824-2>.
- [25] M. Fukuda and G. Gour, *Additive bounds of minimum output entropies for unital channels and an exact qubit formula* (2015), 1502.06411, URL <http://arxiv.org/abs/1502.06411>.
- [26] J. Shamsul Shaari and S. Mancini, ArXiv e-prints (2016), 1603.06189.
- [27] P. O. Boykin and V. Roychowdhury,

- Phys. Rev. A **67**, 042317 (2003), URL <http://link.aps.org/doi/10.1103/PhysRevA.67.042317>.
- [28] A. Ambainis, M. Mosca, A. Tapp, and R. D. Wolf, in *Proceedings of the 41st Annual Symposium on Foundations of Computer Science* (IEEE Computer Society, 2000), pp. 547–553.
- [29] A. Nayak and P. Sen, Quantum Information and Computation **7**, 103 (2007).
- [30] S. Rana, P. Parashar, and M. Lewenstein, Phys. Rev. A **93**, 012110 (2016), URL <http://link.aps.org/doi/10.1103/PhysRevA.93.012110>.
- [31] J.-L. Brylinski and R. Brylinski, Mathematics of Quantum Computation, edited by R. Brylinski and G. Chen, CRC Press (2002), arXiv:quant-ph/0108062, URL [arXiv:quant-ph/0108062](http://arxiv.org/abs/quant-ph/0108062).
- [32] S. S. Bullock, D. P. O’Leary, and G. K. Brennen, Phys. Rev. Lett. **94**, 230502 (2005), URL <http://link.aps.org/doi/10.1103/PhysRevLett.94.230502>.
- [33] M. A. Nielsen, Phys. Rev. A **62**, 052308 (2000), URL <http://link.aps.org/doi/10.1103/PhysRevA.62.052308>.
- [34] J. M. Renes, R. Blume-Kohout, A. J. Scott, and C. M. Caves, Journal of Mathematical Physics **45**, 2171 (2003), ISSN 00222488, quant-ph/0310075, URL <http://dx.doi.org/10.1063/1.1737053>.
- [35] private communication with Huangjun Zhu (2015).
- [36] W. de Launey and D. A. Levin, Cryptography and Communications **2**, 307 (2010), ISSN 1936-2455, URL <http://dx.doi.org/10.1007/s12095-010-0033-z>.
- [37] E. Wakakuwa and M. Murao, ArXiv e-prints (2013), 1310.3991.
- [38] L. Yu and K. Nemoto, Phys. Rev. A **94**, 022320 (2016), URL <http://link.aps.org/doi/10.1103/PhysRevA.94.022320>.
- [39] F. Speelman, ArXiv e-prints (2015), 1511.02839.
- [40] D. Gottesman and I. L. Chuang, Nature **402**, 390 (1999).
- [41] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, Phys. Rev. A **54**, 3824 (1996), arXiv:quant-ph/9604024.
- [42] V. Vedral and M. B. Plenio, Phys. Rev. A **57**, 1619 (1998).
- [43] T.-C. Wei and P. M. Goldbart, Physical Review A **68**, 042307 (2003).
- [44] private communication with Andreas Winter (Dec, 2015).